

SOPHOS

Sophos SafeGuard® PrivateDisk 2.50 Hilfe

Stand: März 2011



Inhalt

1	Überblick	2
2	Erste Schritte	6
3	SafeGuard PrivateDisk Benutzeranwendung	15
4	SafeGuard PrivateDisk Portable.....	35
5	Anwendungsbeispiele	37
6	Zentrale Administration.....	42
7	SafeGuard PrivateDisk OLE Automation Interface	48
8	Technischer Support.....	51
9	Rechtliche Hinweise.....	52

1 Überblick

1.1 Was ist SafeGuard® PrivateDisk?

SafeGuard PrivateDisk schützt verlässlich und transparent sensible Daten auf Notebooks und Desktop Computern, unabhängig von ihrem Speicherort (lokale Festplatten, wechselbare Medien, File Server) - zu jeder Zeit und ohne, dass der Benutzer sich über die Sicherheit seiner Daten Gedanken machen muss.

Secure Virtual Disk-Technology - der elektronische Safe

Erreicht wird dies durch das Erzeugen von so genannten Secure Virtual Disks (PrivateDisk-Laufwerke), die logische Laufwerke darstellen, die die Daten verschlüsselt in einer einzigen großen Datei (den so genannten Volume-Dateien) speichern. Unsere Lösung der Secure Virtual Disk-Technologie kombiniert eine weitgehend benutzerunabhängige Verschlüsselung mit dem gleichzeitigen Schutz mehrerer Dateien in einer Secure Virtual Disk. Sie erzeugt quasi einen "elektronischen Safe" auf einem Rechner, der die kostbaren elektronischen Werte (e-assets) schützt.

Der Benutzer muss sich nur an eine solche Secure Virtual Disk anmelden, um quasi den elektronischen Safe zu öffnen. Dann kann er mit seinen verschlüsselten Daten arbeiten. Die Daten werden automatisch verschlüsselt, wenn sie in einer Secure Virtual Disk gespeichert werden. Ebenso werden die Daten automatisch entschlüsselt, wenn sie zur täglichen Arbeit geöffnet werden. Der Benutzer selbst braucht sich mit der Verschlüsselung seiner Daten nicht mehr zu beschäftigen.

1.2 Vorteile

Durch die Secure Virtual Disk-Technologie werden die Vorteile der Datei- sowie der Disk-Verschlüsselung kombiniert:

- Automatische Verschlüsselung (hohe Transparenz).
- Alle Inhalte und Zusatzinformationen wie Verzeichnisinformationen, Dateiname, -größe und Autor sind verschlüsselt.
- Beim Arbeiten mit verschlüsselten Dateien verbleiben die Daten stets verschlüsselt auf der Festplatte, nur im Arbeitsspeicher liegt der Inhalt im Klartext vor.
- Vertrauliche Daten können gesichert werden, ohne dass eine ganze Festplatte oder Partition verschlüsselt werden muss.

1.2.1 Secure Virtual Disks - PrivateDisk-Laufwerke

Die Virtual Disk Technologie ist eine Methode, mit der sich gegenüber dem Betriebssystem die Existenz von zusätzlichen Laufwerken simulieren lässt. Im Gegensatz zu physikalischen Laufwerken speichert eine Virtual Disk die Daten in einer einzigen großen Datei. Für eine 100 MB große Virtual Disk wird eine 100 MB große Datei auf einem der physikalischen Laufwerke benötigt.

Volume-Dateien können auf allen verfügbaren Laufwerken erzeugt werden. Sie können sich auf Wechselmedien (Disketten, CD-ROM, DVD, ZIP, USB- und Flash-Speicherkarten etc.), auf lokalen Laufwerken und sogar auf Netzwerklaufwerken befinden.

Alle Sektoren-Schreib- und Leseoperationen werden ver- und entschlüsselt. Darum sind immer auch alle Datei- und Verzeichnisinformationen innerhalb einer Virtual Disk mit demselben Schlüssel verschlüsselt. Zur Verschlüsselung wird der AES Algorithmus verwendet.

Die Sicherheit liegt im Schutz des PrivateDisk-Laufwerks. Ohne Zugriffsrechte können Benutzer unter Umständen ganze Volume-Dateien (sofern der Zugriff nicht verhindert wird) löschen und den verschlüsselten Inhalt lesen. Sie sind jedoch nie imstande, die Dateien in Klartext zu lesen. Auch die Verzeichnisstruktur, die innerhalb der Volume-Datei gespeichert wird, bleibt ihnen verborgen.

SafeGuard PrivateDisk schützt den Disk-Schlüssel durch Passwörter (PKCS#5) oder durch öffentliche/private Schlüsselpaare mit Hilfe von Zertifikaten. Benutzer können eine Secure Virtual Disk entweder durch die Eingabe des Passworts öffnen, oder indem sie den zum Zertifikat gehörenden privaten Schlüssel (gespeichert in einer Datei oder auf einer Smartcard), das der Secure Virtual Disk zugeordnet wurde, besitzen.

1.3 Schlüssel aus dem SafeGuard Enterprise Schlüsselring

SafeGuard PrivateDisk erlaubt es, neben Passwörtern und Zertifikaten auch Schlüssel aus dem SafeGuard Enterprise Schlüsselring für den Zugriff auf PrivateDisk-Laufwerke zu verwenden. Ist SafeGuard Enterprise auf dem Computer installiert, können alle Schlüssel im Schlüsselring des Benutzers (von SafeGuard Enterprise zentral erzeugte oder auf dem SafeGuard Enterprise Client lokal erzeugte Schlüssel) verwendet werden.

So kann z. B. mehreren Benutzern einfach Zugriff auf dasselbe PrivateDisk-Laufwerk gewährt werden (z. B. auf einem Netzwerk-Share). Für den Zugriff auf das PrivateDisk-Laufwerk muss auf den Computern der Benutzer nur der zum Erstellen des PrivateDisk-Laufwerks verwendete Schlüssel vorhanden sein. Voraussetzung dafür ist, dass auf beiden Computern die Version 2.30 oder höher von SafeGuard PrivateDisk verwendet wird.

Hinweis: Bitte beachten Sie, dass auf beiden Computern derselbe Schlüssel vorhanden sein muss (z. B. ein SafeGuard Enterprise Gruppenschlüssel). Wenn Sie einen SafeGuard Enterprise Schlüssel verwenden, der nicht im Schlüsselring des Benutzers enthalten ist, kann dieser nicht auf das PrivateDisk-Laufwerk zugreifen.

Wenn Sie einen lokal erzeugten SafeGuard Enterprise Schlüssel verwenden, müssen Sie einem Benutzer, der Zugriff auf das PrivateDisk-Laufwerk haben soll, die Passphrase des Schlüssels mitteilen. Der Empfänger wird beim Öffnen des Archivs automatisch zur Eingabe dieser Passphrase aufgefordert.

1.4 Plattformen

SafeGuard PrivateDisk ist für folgende Betriebssysteme verfügbar:

- Windows XP 32-bit
- Windows Vista 32-bit
- Windows Vista 64-bit
- Windows 7 32-bit
- Windows 7 64-bit

1.5 Versionen

Personal Edition

Die Personal Edition ist ideal für einzelne Benutzer und kleinere Firmen. Sie enthält keine zentrale Verwaltung.

Enterprise Edition

Neben dieser für den persönlichen Gebrauch optimierten Version von SafeGuard PrivateDisk bieten wir Ihnen auch eine Enterprise Edition dieses Produkts an. Diese Version ist für größere Unternehmen optimal, die die Software zentral verwalten wollen. Die Enterprise Edition enthält alle Funktionen der Personal Edition plus:

- Zentrale, einfache Konfiguration analog zu anderen SafeGuard Produkten und Windows selbst.
- Eine Auswertung von Certificate Revocation Lists (CRLs) bei der Überprüfung von Zertifikaten.

Da die Installation von SafeGuard PrivateDisk mit Hilfe des Windows Installer erfolgt, kann eine Installation ohne Benutzereingriff mittels der Windows Standardmechanismen ausgeführt werden.

Ein Upgrade von der Personal Edition zur Enterprise Edition von SafeGuard PrivateDisk ist ohne Probleme möglich, umgekehrt jedoch nicht.

Demo-Version

Eine Demo-Version von SafeGuard PrivateDisk steht auf <http://www.sophos.com/products/enterprise/encryption/safeguard-privatedisk/> zum kostenlosen Download zur Verfügung.

Bei dieser Version handelt es sich um eine voll funktionsfähige Personal Edition zu Evaluationszwecken, die 30 Tage ohne Einschränkungen verwendet werden kann. Danach haben Sie nur mehr lesenden Zugriff auf PrivateDisk-Laufwerke bis Sie das Produkt im Sophos Webshop gekauft haben. Zusätzlich wird ein Begrüßungsbildschirm angezeigt, bis das gekauft wird.

Upgrade der Demo-Version

Wenn Sie einen Upgrade von einer Demo Version auf eine Vollversion von SafeGuard PrivateDisk durchführen wollen, müssen Sie nur die Vollversion über die bestehende Demo-Version von SafeGuard PrivateDisk installieren. Die Demo-Version kann mit beiden Versionen von SafeGuard PrivateDisk aktualisiert werden.

1.5.1 Upgrade auf Version 2.50

Ein Upgrade von bestehenden Versionen auf die Version 2.50 ist ohne Probleme möglich. Bestehende PrivateDisk-Laufwerke (die Volume-Dateien) können mit der neuen Version weiter verwendet werden.

Hinweis: Beginnend mit Version 2.00 verwendet SafeGuard PrivateDisk standardmäßig den AES-256 Algorithmus, während ältere Versionen AES-128 verwendet haben (AES-256 wurde nicht unterstützt). Wenn Sie mit der Version 2.50 Volume-Dateien erzeugen wollen, die auch von älteren SafeGuard PrivateDisk Versionen verwendet werden sollen, müssen Sie beim Anlegen des PrivateDisk-Laufwerks den Verschlüsselungsalgorithmus AES-128 explizit auswählen. PrivateDisk-Laufwerke, die AES-256 verwenden, können zusammen mit älteren Versionen nicht verwendet werden.

2 Erste Schritte

2.1 Zertifikate

SafeGuard PrivateDisk erlaubt es, Zertifikate und Public Key Schlüsselpaare, anstelle von Passwörtern zu verwenden. Wird ein Zertifikat einem PrivateDisk-Laufwerk zugewiesen, kann es zur Authentisierung verwendet werden. Nur der Besitzer des Zertifikats hat Zugriff auf den zum Zertifikat gehörenden privaten Schlüssel und kann es daher zur Anmeldung an das PrivateDisk-Laufwerk verwenden. Analog zu Passwörtern können Zertifikate mit Benutzerrechten oder Administratorrechten ausgestattet werden.

Im Folgenden erhalten Sie einige wichtige Vorabinformationen für die Verwendung von Zertifikaten:

SafeGuard PrivateDisk verwendet das Microsoft Crypto API ausschließlich für die Zertifikatsfunktionalität. Für die Verschlüsselung des PrivateDisk-Laufwerks wird eine eigene Implementierung von AES und SHA-1 verwendet.

SafeGuard PrivateDisk unterstützt alle Cryptographic Service Provider (CSP), z. B. Microsoft Enhanced CSP.

Für das höchstmögliche Sicherheitsniveau empfehlen wir die Verwendung von starken CSPs, wie den Microsoft Strong Cryptographic Service Provider (benötigt Windows XP oder das Microsoft High Encryption Pack). Diese CSPs erlauben die Verwendung von Schlüssellängen bis zu 4096 bit und bieten starke Verschlüsselungsalgorithmen (wie 3DES).

Vorbedingungen zur Verwendung von Zertifikaten mit SafeGuard PrivateDisk:

- Das Zertifikat muss einen öffentlichen Schlüssel enthalten.
- Um Zugriff auf ein PrivateDisk-Laufwerk über ein Zertifikat zu erhalten, muss der private Schlüssel des zugewiesenen Zertifikats verfügbar sein.
- Nur Zertifikate, die unter *Benutzerkonfiguration* im Zertifikatsspeicher **Eigene Zertifikate**, **Adressbuch** und **Andere Personen** sowie unter *Richtlinien für Lokaler Computer* im Zertifikatsspeicher **Eigene Zertifikate** gespeichert sind, werden von SafeGuard PrivateDisk aufgelistet. Zertifikate, die an anderen Orten gespeichert sind, werden von SafeGuard PrivateDisk nicht berücksichtigt.
Zertifikate können mit dem Zertifikate Snap-In für die Management Konsole importiert und verwaltet werden.
- Zum Hinzufügen eines Zertifikats zu einem PrivateDisk-Laufwerk, wird nur der öffentliche Schlüssel verwendet. Der private Schlüssel muss nicht bekannt sein. Der private Schlüssel bleibt immer im Eigentum des Besitzers und nur dieser ist dann imstande dieses PrivateDisk-Laufwerk zu öffnen.

Es ist empfehlenswert, die Zertifikate zur Verfügung zu haben, bevor die Installation von SafeGuard PrivateDisk begonnen wird. Auf diese Weise werden sie sofort nach der Installation im Dialog *Zertifikate hinzufügen* angezeigt und können jedem PrivateDisk-Laufwerk zugewiesen werden.

Hinweis: Die Verwaltung von Zertifikaten ist keine Aufgabe von PrivateDisk. Die Zertifikatsverwaltung kann mittels einer firmeneigenen PKI-Infrastruktur oder mittels eines Trust Centers durchgeführt werden.

2.1.1 Zertifikatsprüfung

Zertifikate zur Verwendung in SafeGuard PrivateDisk müssen folgenden Anforderungen genügen:

- SafeGuard PrivateDisk überprüft die Gültigkeitsdauer eines Zertifikats. Zertifikate, deren Gültigkeitsdauer abgelaufen ist, können zur Anmeldung verwendet werden, jedoch können sie nicht einem PrivateDisk-Laufwerk zugeordnet werden.
- Die kritischen Zertifikatserweiterungen werden überprüft. Zertifikate mit unbekanntem kritischen Erweiterungen können nicht zugewiesen werden. Dieses Default-Verhalten kann in der Enterprise Edition über die administrative Vorlage geändert werden.
- Reine Signatur-Zertifikate können nicht zugewiesen werden. Dieses Default-Verhalten kann in der Enterprise Edition über die administrative Vorlage geändert werden.

Enterprise Edition

- Die Enterprise Edition von SafeGuard PrivateDisk erlaubt es, eine erweiterte Zertifikatsprüfung durchzuführen. Dies bedeutet, dass Zertifikate nur akzeptiert werden, wenn Sie vollständig überprüft werden können (Auswertung einer Certificate Revocation List). Hierzu muss bei Bedarf eine CRL des Ausstellers über das Netzwerk geladen werden. Kann das Zertifikat nicht überprüft werden, wird die Anmeldung an ein PrivateDisk-Laufwerk verweigert. Diese erweiterte Zertifikatsprüfung ist standardmäßig deaktiviert.

Hinweis: Bitte beachten Sie, dass zur Auswertung einer CRL eine Netzwerkverbindung notwendig sein kann. Kann die Verbindung nicht hergestellt werden, so wird der Zugriff verweigert, auch wenn das Zertifikat eigentlich gültig wäre.

- In der Enterprise Edition kann ein bevorzugter CSP definiert werden. Wenn ein Benutzer ein neues Laufwerk mit einem Passwort oder einem Zertifikat von einem anderen CSP absichern will, dann wird er darauf hingewiesen, dass Zertifikate des bevorzugten CSP sicherer wären.

2.1.2 Smartcard Leser

Da die Benutzung von Zertifikaten durch die Verwendung von Cryptographic Service Provider abgewickelt wird, werden Smartcard-Leser automatisch unterstützt, wenn ein Smartcard CSP verwendet wird. Die Anmeldung an ein PrivateDisk-Laufwerk kann daher durch ein auf Smartcard gespeichertes Zertifikat abgewickelt werden.

Wenn Sie Zertifikate auf Smartcards zur Anmeldung an ein PrivateDisk-Laufwerk verwenden wollen, stellen Sie bitte sicher, dass der Smartcard Leser und ein entsprechender Cryptographic Service Provider korrekt installiert sind!

2.2 Installation

Hinweis: Die Installation von SafeGuard PrivateDisk ist nur möglich, wenn Sie mit Administratorrechten an das Betriebssystem angemeldet sind.

Wenn Sie das Programm aus dem Internet heruntergeladen haben, starten Sie einfach diese Datei.

Benutzen Sie eine SafeGuard PrivateDisk Programm-CD, wird die Installation nach dem Einlegen der CD in das CD-ROM Laufwerk automatisch gestartet (sollte dies nicht der Fall sein, klicken Sie auf die **.exe-** bzw. **.msi-Datei** im **Install** Verzeichnis der Installations-CD).

Ein Installations-Assistent führt Sie durch die sehr einfache Installation von SafeGuard PrivateDisk.

Aktivieren Sie die Option **Ich akzeptiere die Lizenzvereinbarung** im Dialog *Lizenzvereinbarung*. Wenn Sie dies nicht tun, ist eine Installation von SafeGuard PrivateDisk nicht möglich!

SafeGuard PrivateDisk ist unmittelbar nach der Installation einsatzbereit.

2.2.1 Tray Icon

SafeGuard PrivateDisk platziert ein Symbol in der Windows Taskleiste. Ein Rechtsklick auf dieses Symbol zeigt ein Menü mit Einträgen

- für das Starten der Benutzeranwendung (**Private Disk**),
- zum Starten eines Assistenten zum Anlegen neuer Laufwerke (**Neues Laufwerk**),
- zum Importieren von Laufwerken (**Laufwerk importieren**),
- zum Anmelden/Abmelden an ein PrivateDisk-Laufwerk (**Anmelden/Abmelden**),
- zum Definieren bestimmter Einstellungen für SafeGuard PrivateDisk (**Optionen**). Auf diese Einstellungen haben Sie nur Zugriff, wenn Sie als Administrator an das System angemeldet sind.

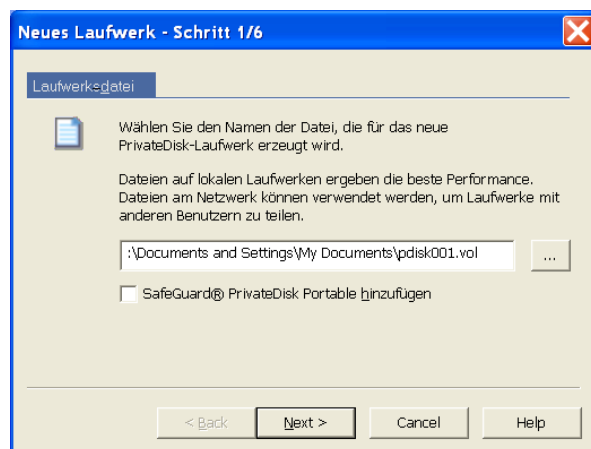
Die SafeGuard PrivateDisk Benutzeranwendung kann auch durch Klicken auf **Start/Programme/Sophos/SafeGuard PrivateDisk** gestartet werden.

2.3 Schnellstart

Benutzen Sie nach der Installation den Assistenten *Neues Laufwerk* zur Erstellung eines PrivateDisk-Laufwerks. Dieser Assistent führt Sie in sechs einfachen Schritten durch die Erstellung eines PrivateDisk-Laufwerks.

Danach können Sie das neue PrivateDisk-Laufwerk wie ein zusätzliches Laufwerk Ihres Computers benutzen. Die Daten auf dem neuen Laufwerk werden automatisch ver- bzw. entschlüsselt.

Um ein neues PrivateDisk-Laufwerk zu erstellen, klicken Sie mit der rechten Maustaste auf das SafeGuard PrivateDisk Symbol in der Windows Taskleiste. Klicken Sie anschließend auf **Neues Laufwerk**. Der Assistent zum Anlegen eines neuen PrivateDisk-Laufwerks wird gestartet.



1. Geben Sie den Pfad und den Dateinamen für das zu erzeugende PrivateDisk-Laufwerk an. Die Dateierweiterung .vol kennzeichnet die neue Volume-Datei.

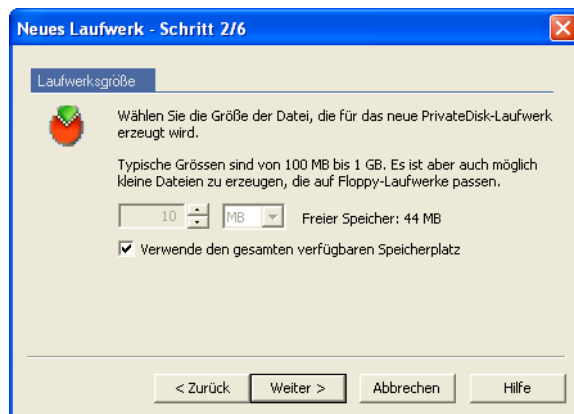
Die Pfade unter denen PrivateDisk-Laufwerke angelegt werden dürfen können durch eine zentrale Einstellung eingeschränkt werden. Wenn Sie ein Laufwerk an einem nicht erlaubten Speicherort anlegen wollen, wird ein Hinweis angezeigt, welche Pfade erlaubt sind.

- **SafeGuard PrivateDisk Portable hinzufügen**

Wenn Sie diese Option aktivieren, wird SafeGuard PrivateDisk Portable zusätzlich zur .vol-Datei auf das Medium kopiert.

SafeGuard PrivateDisk Portable ermöglicht das Öffnen von PrivatrDisk-Laufwerken auf Computern ohne SafeGuard PrivateDisk.

Klicken Sie auf **Weiter**.



2. Wählen Sie die Größe Ihres neuen SafeGuard PrivateDisk-Laufwerks. Typische Größen liegen zwischen 100 MB und 1 GB.

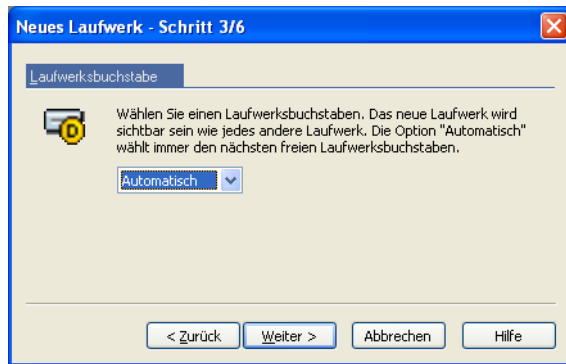
- **Verwende den gesamten verfügbaren Speicherplatz**

Wenn Sie diese Option aktivieren, verwendet SafeGuard PrivateDisk den gesamten auf dem ausgewählten Laufwerk zur Verfügung stehenden Speicherplatz für das neue PrivateDisk-Laufwerk. Der verfügbare Speicherplatz wird unter *Freier Speicher*: angezeigt.

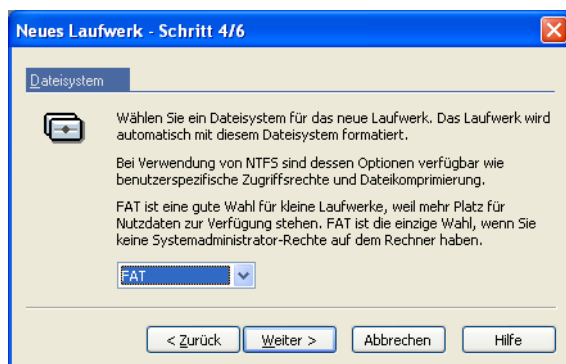
Die maximale Größe eines PrivateDisk-Laufwerks kann durch eine zentrale Einstellung beschränkt werden. Wenn Sie ein größeres Laufwerk als erlaubt anlegen wollen, wird ein Hinweis angezeigt, wie groß ein PrivateDisk-Laufwerk maximal sein darf.

Klicken Sie auf **Weiter**.

Hinweis: Die Größe eines PrivateDisk-Laufwerks kann nach dem Anlegen nicht mehr geändert werden. Sollten Sie mehr Speicherplatz benötigen, müssen Sie ein neues Laufwerk anlegen und die Daten vom Originallaufwerk in das neue Laufwerk kopieren.

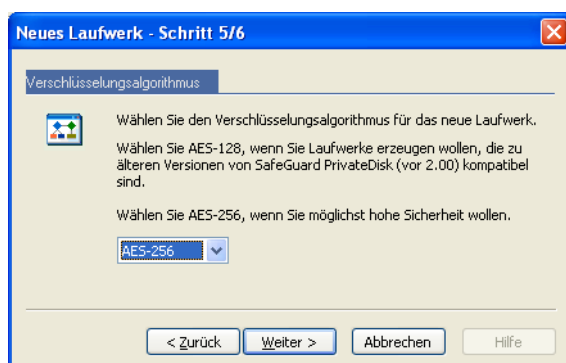


3. Wählen Sie einen Laufwerksbuchstaben für das neue SafeGuard PrivateDisk-Laufwerk. Das neue Laufwerk wird wie jedes andere lokale Laufwerk angezeigt. Die Option **Automatisch** wählt immer den nächsten freien Laufwerksbuchstaben. Klicken Sie auf **Weiter**.



4. Wählen Sie ein Dateisystem für Ihr neues SafeGuard PrivateDisk-Laufwerk aus. Das Laufwerk wird automatisch formatiert. Klicken Sie auf **Weiter**.

Hinweis: Benutzer, die ohne Administratorrechte an das Betriebssystem angemeldet sind, können nur FAT als Dateisystem für das PrivateDisk-Laufwerk auswählen.



5. Wählen Sie einen Verschlüsselungsalgorithmus für das neue Laufwerk aus. Sie können zwischen AES-128 und AES-256 wählen.

Hinweis: Beginnend mit Version 2.00 verwendet SafeGuard PrivateDisk standardmäßig den AES-256 Algorithmus, während ältere Versionen AES-128 verwendet haben (AES-256 wurde nicht unterstützt). Wenn Sie mit der Version 2.30 Volume-Dateien erzeugen wollen, die auch von älteren SafeGuard PrivateDisk Versionen verwendet werden sollen, müssen Sie beim Anlegen des PrivateDisk-Laufwerks den Verschlüsselungsalgorithmus AES-128 explizit auswählen. PrivateDisk-Laufwerke, die AES-256 verwenden, können zusammen mit älteren Versionen nicht verwendet werden.

Klicken Sie auf **Weiter**.

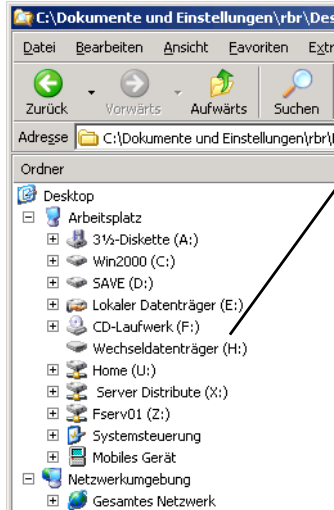


6. Wählen Sie:

- Ein **Administrator-Passwort** für Ihr neues SafeGuard PrivateDisk-Laufwerk und bestätigen Sie es. Das Passwort wird jedesmal überprüft, wenn Sie sich an ein PrivateDisk-Laufwerk anmelden.
- **Einen SafeGuard Enterprise Schlüssel**
Ist SafeGuard Enterprise oder SafeGuard RemovableMedia auf Ihrem Computer installiert, können Sie einen Schlüssel aus deren Schlüsselring verwenden. Dieser Schlüssel wird zum Erzeugen und Anmelden an ein PrivateDisk-Laufwerk verwendet. Es ist kein zusätzliches Passwort notwendig.
- **Verwende mein Zertifikat zur Administration des Laufwerks**
Wird diese Option aktiviert, kann ein Zertifikat des Benutzers an Stelle des Administrator-Passworts angegeben werden. Diese Option ist nur aktiviert, wenn ein Zertifikat (privater Schlüssel) vorhanden ist.
Ist mehr als ein Zertifikat vorhanden, wird ein Dialog angezeigt, in dem ein Zertifikat ausgewählt werden kann.

7. Klicken Sie auf **Fertig stellen**.

SafeGuard PrivateDisk legt das neue PrivateDisk-Laufwerk an.



Wenn Sie an die Secure Virtual Disk angemeldet sind, wird sie wie jedes andere Laufwerk Ihres Systems angezeigt. Sie kann wie ein „normales“ Laufwerk benutzt werden. Die Daten werden automatisch ver- und entschlüsselt.

Wenn Sie sich von der Secure Virtual Disk abmelden (Rechtsklick im Explorer), wird das Laufwerk geschlossen und wird aus der Liste der verfügbaren Laufwerke entfernt.

2.4 Installation ohne Benutzerinteraktion

Die Installation ohne Benutzerinteraktion erlaubt die automatische Installation von SafeGuard PrivateDisk auf einer großen Zahl von Rechnern.

Das Verzeichnis `Install` Ihrer Installations-CD enthält die Datei `sgpd100_german.msi`, die für die Installation ohne Benutzerinteraktion unbedingt notwendig ist.

2.4.1 Kommandozeilensyntax

Zum Ausführen einer Installation ohne Benutzerinteraktion muss `msiexec` mit bestimmten Parametern aufgerufen werden.

Unbedingt erforderliche Parameter:

`/I`

Gibt das Installations-Package an, das zu installieren ist.

`/QN`

Installation ohne Benutzerinteraktion.

Name der `.msi` Datei: `sgpd100_german.msi`

Syntax:

```
msiexec /i <path>\sgpd100_german.msi /qn
```

Optionale Parameter:

/L* <Pfad + Dateiname>

Protokolliert alle Warnungen und Fehlermeldungen in der unter <Pfad + Dateiname> angegebenen Datei.

Beispiel:

```
msiexec /i C:\Install\sgpd100_german.msi /qn
```

Die Installation von SafeGuard PrivateDisk wird ausgeführt. Das Programm wird im Standardverzeichnis (<Systemlaufwerk>:\ Programme\Sophos) installiert.

Die .msi Datei befindet sich im Verzeichnis Install auf Laufwerk C.

3 SafeGuard PrivateDisk Benutzeranwendung

Die SafeGuard PrivateDisk Benutzeranwendung kann durch einen Rechtsklick auf das Symbol in der Windows Taskleiste und einem anschließenden Klick auf **PrivateDisk** gestartet werden. Es ist auch möglich, das Programm über **Start/Programme/Sophos/SafeGuard PrivateDisk** zu starten.



Der linke Teil der Benutzeranwendung zeigt eine Liste aller verfügbaren PrivateDisk-Laufwerke an.

Wird im linken Fenster ein PrivateDisk-Laufwerk ausgewählt, werden im rechten Fenster der Benutzeranwendung Details über diese Disk angezeigt. Ist keine Disk ausgewählt, z. B. nach dem Start der Benutzeranwendung, wird ein Willkommensbildschirm angezeigt, der Informationen über grundlegende Funktionen (Erzeugen neuer verschlüsselter Laufwerke, Laufwerke importieren) enthält.

Wird im linken Fenster ein PrivateDisk-Laufwerk ausgewählt und die **Entf**-Taste gedrückt (bzw. auf **Bearbeiten/Aus der Liste herausnehmen** geklickt), wird die Disk aus der Liste der zur Verfügung stehenden Disks entfernt. Die Volume-Datei ist aber immer noch vorhanden und kann durch Importieren wieder in die Liste aufgenommen werden.

Um ein PrivateDisk-Laufwerk zu löschen (die Volume-Datei tatsächlich löschen), wählen Sie dieses aus und klicken Sie anschließend auf **Löschen** im Menü *Bearbeiten*. Danach wird ein Dialog angezeigt, der Sie informiert, dass alle im Laufwerk gespeicherten Daten verloren gehen. Wenn Sie diesen mit **Ja** bestätigen, wird die Volume-Datei gelöscht.

3.1 Symbolleiste und Menükommandos

SafeGuard PrivateDisk bietet eine Symbolleiste mit Schaltflächen für die wichtigsten Kommandos:



- **Neu:**
Startet den Assistenten zum Anlegen eines neuen PrivateDisk-Laufwerks.
- **Anmelden:**
Anmelden an ein PrivateDisk-Laufwerk.
- **Abmelden:**
Abmelden von einem PrivateDisk-Laufwerk.
- **Passwörter:**
Zeigt den Dialog *Passwort ändern* zum Ändern bzw. Setzen von Passwörtern (Administrator oder Benutzer) für ein PrivateDisk-Laufwerk an.
- **Zertifikate:**
Zeigt den Dialog *Zertifikate* zum Hinzufügen und Administrieren von Zertifikaten für PrivateDisk-Laufwerke, an.
- **Optionen:**
Zeigt den Dialog *Optionen* zum Ändern der Einstellungen für SafeGuard PrivateDisk an. Diese Option steht nur Benutzern mit Administratorrechten zur Verfügung.
- **Hilfe:**
Zeigt die SafeGuard PrivateDisk Online Hilfe an.

Um Zugriff auf die wichtigsten Funktionen von SafeGuard PrivateDisk zu erhalten (und um die Benutzeranwendung zu starten), kann auch das SafeGuard PrivateDisk-Symbol in der Windows-Taskleiste verwendet werden.

3.2 Informationen über das ausgewählte PrivateDisk-Laufwerk

Wird im linken Fenster ein PrivateDisk-Laufwerk ausgewählt, werden im rechten Fenster detaillierte Informationen über diese Disk angezeigt.

■ Name:

Jedes Laufwerk kann einen symbolischen Namen besitzen. Der Standardname ist der Name der Volume-Datei ohne Pfadangabe. Der Standardname kann in diesem Dialog geändert werden.

Zum Ändern des Namens geben Sie eine neue Bezeichnung für das Laufwerk in das Eingabefeld ein und drücken Sie anschließend auf Enter. Der neue Name wird in der Liste der zur Verfügung stehenden Laufwerke angezeigt. Der Name ist nur für diese Liste gültig. Im Windows Explorer wird jedes PrivateDisk-Laufwerk als `Wechseldatenträger (Laufwerksbuchstabe:)` angezeigt.

■ Status:

Zeigt den aktuellen Status des PrivateDisk-Laufwerks.

- **Angemeldet:** Der Benutzer ist an das PrivateDisk-Laufwerk angemeldet und das Laufwerk ist verfügbar.

In Klammern wird angezeigt, mit welchen Rechten (Administrator, Benutzer oder Benutzer, nur lesen) der Benutzer angemeldet ist.

- **Abgemeldet:** Es ist kein Benutzer an das PrivateDisk-Laufwerk angemeldet.
- **Datei nicht gefunden:** Die angegebene Volume-Datei existiert nicht (z. B. wenn die Datei umbenannt, verschoben oder gelöscht wurde).
- **Kein PrivateDisk-Laufwerk:** Die ausgewählte Datei ist keine gültige Volume-Datei.
- **Zugriff verweigert:** Der Zugriff auf die Volume-Datei wird verweigert, z. B. aufgrund von fehlenden NTFS Rechten.

■ Datei:

Zeigt den Namen und den Pfad jener Datei an, in der die Daten für das PrivateDisk-Laufwerk gespeichert werden.

■ Laufwerk:

Zeigt den aktuellen Laufwerksbuchstaben des PrivateDisk-Laufwerks an und erlaubt es, diesen zu ändern.

Laufwerksbuchstaben können entweder fix vergeben werden (von A bis Z) oder es wird die Option **Automatisch** gewählt. In diesem Fall wird bei der Anmeldung der nächste freie Laufwerksbuchstabe verwendet.

Der Laufwerksbuchstabe kann vom Benutzer zu jeder Zeit geändert werden. Änderungen werden aktiv, wenn sich der Benutzer das nächste Mal an das PrivateDisk-Laufwerk anmeldet. Aus diesem Grund wird der Benutzer bei der Änderung des Laufwerksbuchstaben gefragt, ob er eine Neuanschaltung durchführen will. Klicken Sie auf **Ja**, damit die Änderungen sofort übernommen werden.

■ **Start:**

Legt fest, wie und wann die Anmeldung an das ausgewählte PrivateDisk-Laufwerk durchgeführt werden soll. Folgende Optionen stehen zur Verfügung:

■ **Manuell anmelden**

Die Anmeldung erfolgt nicht automatisch. Der Benutzer muss sich jedesmal manuell anmelden, wenn er das Laufwerk benutzen will.

■ **Anmelden, wenn der Benutzer sich ans System anmeldet**

Die Anmeldung erfolgt automatisch, sobald sich der Benutzer an das Betriebssystem anmeldet.

Hinweis: Wenn die Option **Anmelden, wenn der Benutzer sich ans System anmeldet** ausgewählt wird, muss auch die Option **Automatischer Logon beim Starten** auf der Seite **Allgemein** des Optionendialogs ausgewählt werden.

■ **Anmelden, wenn Laufwerksdatei verfügbar ist**

Die Anmeldung erfolgt automatisch, wenn die Volume-Datei für das Laufwerk verfügbar ist. Diese Option ist für PrivateDisk-Laufwerke auf Netzwerklaufwerken und Plug&Play-Geräten gedacht.

■ **Anmelden, wenn Smartcard eingesteckt wird**

Die Anmeldung erfolgt automatisch, wenn die Smartcard in den Kartenleser gesteckt wird.

Hinweis: Wenn diese Option ausgewählt wird, muss auf der Seite **Smartcard** im Optionendialog ein Kartenleser ausgewählt werden.

■ **Attribute:**

Erlaubt es, Optionen für die Anmeldung an ein PrivateDisk-Laufwerk zu definieren.

■ **Nur Lesen:**

Ist diese Option aktiviert, wird das PrivateDisk-Laufwerk bei der Anmeldung immer ausschließlich mit Leserechten für den Benutzer geöffnet, auch wenn der Benutzer eigentlich Lese- und Schreibrechte auf die Volume-Datei hätte.

Mit Schreibrechten kann immer nur ein einziger Benutzer an ein PrivateDisk-Laufwerk angemeldet sein. Das Attribut **Nur Lesen** kann verwendet werden, um gleichzeitig weiteren Benutzern Zugriff auf ein PrivateDisk-Laufwerk zu ermöglichen.

Änderungen, die der schreibende Benutzer durchführt, werden mit kurzer Verzögerung bei den anderen Benutzern sichtbar.

- **Simuliere Festplatte:**

Wird diese Option ausgewählt, simuliert SafeGuard PrivateDisk kein Wechsellaufwerk, sondern eine Festplatte - die Anzeige im Windows Explorer ändert sich entsprechend. Damit ein PrivateDisk-Laufwerk freigegeben werden kann, muss diese Option aktiviert sein.

Laufwerke können nur freigegeben werden, wenn Sie mit Administratorrechten an das Betriebssystem angemeldet sind.

- **Größe:**

Zeigt die Größe des PrivateDisk-Laufwerks an.

Neben der Größe wird der Algorithmus, der zur Verschlüsselung verwendet wird, angezeigt.

Hinweis: Mit AES-256 verschlüsselte Laufwerke können in SafeGuard PrivateDisk Versionen vor 2.00 nicht verwendet werden.

- **Passwörter:**

Unter *Passwörter* wird angezeigt, welche Passwörter für das PrivateDisk-Laufwerk vergeben wurden. Ein PrivateDisk-Laufwerk kann ein Administrator-Passwort oder ein Administrator- und ein Benutzer-Passwort oder nur ein Benutzer-Passwort haben, wenn ein Zertifikat mit Administratorrechten zugewiesen wurde (siehe Seite 28).

- **Zertifikate:**

Unter *Zertifikate* wird eine Liste mit allen Zertifikaten, die dem PrivateDisk-Laufwerk zugeordnet sind, angezeigt. Für jedes Zertifikat werden Status (Administrator oder Benutzer) und Rechte (Nur Lesen oder Lesen und Schreiben) angezeigt.

Nur mit Administratorrechten ist es möglich, die Liste der zugewiesenen Zertifikate zu ändern.

3.3 Erzeugen eines neuen PrivateDisk-Laufwerks

Neue PrivateDisk-Laufwerke können auf folgende Arten erzeugt werden:

- Durch Klicken auf die Schaltfläche **Neues Laufwerk** im *Willkommen* Dialog.
- Durch Klicken auf die Schaltfläche **Neu** in der SafeGuard PrivateDisk-Symbolleiste.
- Durch Klicken auf **Neu** im Menü *Datei*.
- Durch Klicken auf **Neues Laufwerk** im Kontextmenü des SafeGuard PrivateDisk-Symbols in der Windows-Taskleiste.

In allen Fällen wird der Assistent zur Erstellung eines neuen Laufwerks gestartet.

3.4 Anmeldung und Abmeldung an ein PrivateDisk-Laufwerk

Um Zugriff auf ein PrivateDisk-Laufwerk zu haben, muss sich ein Benutzer anmelden. Um sich anmelden zu können, muss der Benutzer im Besitz eines Passworts für das Laufwerk sein, oder er besitzt den privaten Schlüssel eines Zertifikats, das dem Laufwerk zugewiesen ist, oder er verfügt über den SafeGuard Enterprise Schlüssel, der zum Erzeugen des Laufwerks verwendet wurde.

Zum Anmelden an ein bzw. Abmelden von einem PrivateDisk-Laufwerk:

- Wählen Sie das PrivateDisk-Laufwerk aus und klicken Sie auf **Anmelden** bzw. **Abmelden** in der SafeGuard PrivateDisk-Symbolleiste.
- Wählen Sie das PrivateDisk-Laufwerk aus und klicken Sie auf **Anmelden/Abmelden/Alle Laufwerke abmelden** im Menü *Bearbeiten*.
- Klicken Sie auf das SafeGuard PrivateDisk-Symbol in der Windows-Taskleiste. Wenn Sie auf **Anmelden** bzw. **Abmelden** klicken, können Sie das entsprechende Laufwerk auswählen.
- Wählen Sie die Volume-Datei im Windows Explorer aus und klicken Sie auf **Anmelden** bzw. **Abmelden** im SafeGuard PrivateDisk-Kontextmenü.

Wenn sich ein Benutzer nicht an ein Laufwerk anmelden kann, weil es bereits von einem anderen Benutzer verwendet wird, wird als Hinweis der Name dieses anderen Benutzers angezeigt.

Wenn sich ein Benutzer nicht von einem Laufwerk abmelden kann, weil es noch von Programmen benutzt wird, wird ein Dialog angezeigt, der folgende Optionen bietet:

- **Wiederholen**
Meldet den Benutzer vom Laufwerk ab, nachdem entsprechende Programme bzw. Dateien geschlossen wurden.
- **Abmeldung erzwingen**
Meldet den Benutzer ab, auch wenn das Laufwerk noch verwendet wird.
Achtung:
Hierbei kann es zu Datenverlust kommen!
- **Abbrechen**
Der Benutzer bleibt an das Laufwerk angemeldet.

3.5 Importieren eines PrivateDisk-Laufwerks

Wenn Sie ein PrivateDisk-Laufwerk verwenden wollen, das noch nicht in der Liste der verfügbaren Laufwerke erscheint, können Sie den Befehl **Importieren** aus dem Menü *Datei* verwenden, um es der Liste der verfügbaren Laufwerke hinzuzufügen.

Es wird ein Dialog geöffnet, in dem Sie die Laufwerksdatei auswählen können. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**. Das Laufwerk wird in die Liste der verfügbaren Laufwerke aufgenommen.

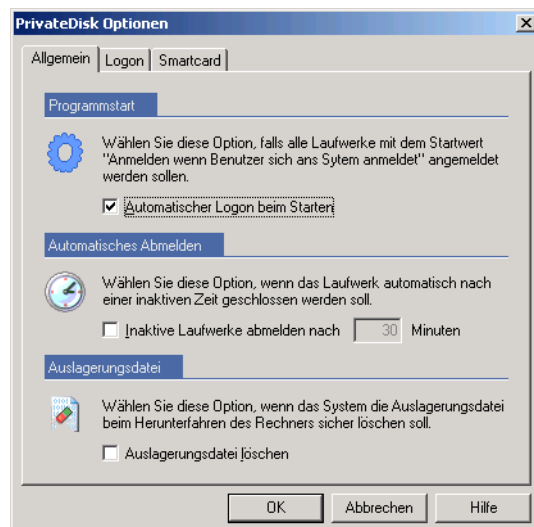
3.6 SafeGuard PrivateDisk® Optionen

SafeGuard PrivateDisk bietet verschiedene Optionen, um das Produkt den jeweiligen persönlichen Bedürfnissen anzupassen. Diese Einstellungen können im Dialog *PrivateDisk Optionen* vorgenommen werden. Öffnen Sie diesen Dialog, indem Sie auf die Schaltfläche **Optionen** in der SafeGuard PrivateDisk Symbolleiste klicken (bzw. auf **Optionen** im Menü *Extras*). Der Dialog *PrivateDisk Optionen* kann auch durch einen Rechtsklick auf das SafeGuard PrivateDisk-Symbol in der Windows-Taskleiste und anschließendes Klicken auf **Optionen** geöffnet werden.

Der Dialog *PrivateDisk Optionen* besteht aus drei verschiedenen Seiten:

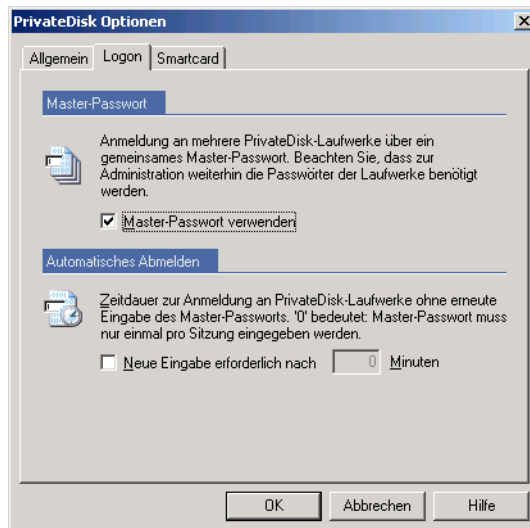
3.6.1 Die Seite Allgemein

Diese Seite enthält generelle Optionen, die das Verhalten von SafeGuard PrivateDisk bestimmen.



- **Automatischer Logon beim Starten:**
Wenn diese Option aktiviert ist, wird der Benutzer an alle SafeGuard PrivateDisk-Laufwerke mit der Start-Option **Anmelden, wenn der Benutzer sich ans System anmeldet** automatisch angemeldet, sobald er sich an das Betriebssystem anmeldet.
Abhängig von der Einstellung auf der Seite *Logon* (Master-Passwort verwenden oder nicht) führt dies dazu, dass für jedes Laufwerk ein Passwort eingegeben werden muss, oder es wird ein einzelner Dialog angezeigt, in dem ein Master-Passwort für alle PrivateDisk-Laufwerke eingegeben werden muss.
- **Inaktive Laufwerke abmelden nach:**
Wird diese Option aktiviert, werden Laufwerke geschlossen, nachdem sie für die angegebene Zeitdauer nicht benutzt wurden.
- **Auslagerungsdatei löschen:**
Da die Auslagerungsdatei sensible Daten enthalten kann, bietet SafeGuard PrivateDisk die Möglichkeit, diese Datei beim Herunterfahren des Systems sicher zu löschen.
Wird diese Option aktiviert, wird die Auslagerungsdatei beim Herunterfahren sicher gelöscht und stellt damit kein Sicherheitsrisiko mehr dar.

3.6.2 Die Seite Logon



- **Master-Passwort verwenden:**
Wenn ein Benutzer mehrere PrivateDisk-Laufwerke verwendet, muss er bei der Anmeldung für jedes Laufwerk das entsprechende Passwort eingeben.
Um diesen Vorgang zu vereinfachen, bietet SafeGuard PrivateDisk die Möglichkeit, ein Master-Passwort zu verwenden. Ist diese Option aktiviert, wird ein Master-Passwort zur sicheren Speicherung der einzelnen Passwörter für die PrivateDisk-Laufwerke verwendet. Der Benutzer muss dann nur das Master-Passwort eingeben und nicht die Passwörter für jedes einzelne Laufwerk.

Die Passwörter für die einzelnen PrivateDisk-Laufwerke werden gespeichert, sobald sie das erste Mal eingegeben werden, nachdem die Option **Master-Passwort verwenden** aktiviert wurde.

Zum Ändern des Master-Passworts, verwenden Sie bitte das Kommando **Master-Passwort ändern** aus dem Menü *Extras*.

Um zu vermeiden, dass der Benutzer wiederholt nach dem Master-Passwort gefragt wird, kann das Master-Passwort für eine konfigurierbare Zeitspanne gespeichert werden.

■ **Neue Eingabe erforderlich nach:**

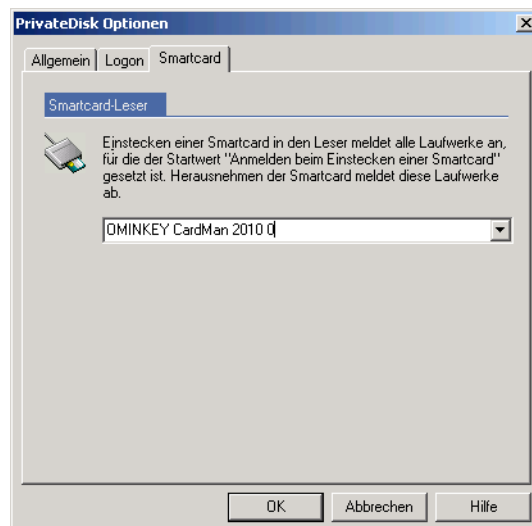
Ist diese Option aktiviert, kann eine Zeitspanne (in Minuten) angegeben werden, für die das Master-Passwort im Speicher behalten wird. Danach wird das Master-Passwort aus dem Speicher gelöscht.

Hinweis: Für die Anmeldung mit Zertifikaten ist die Master-Passwort Funktionalität nicht verfügbar.

3.6.3 Die Seite Smartcard

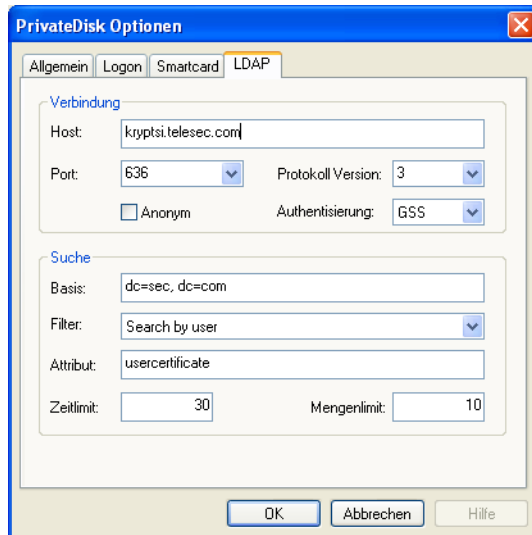
Wird eine Smartcard in den Kartenleser eingelegt, wird der Benutzer automatisch an SafeGuard PrivateDisk-Laufwerke, für die die Start-Option **Anmelden, wenn Smartcard eingesteckt wird** gewählt wurde, angemeldet.

Wird die Smartcard aus dem Kartenleser entfernt, wird der Benutzer von allen PrivateDisk-Laufwerken mit der Start-Option **Anmelden, wenn Smartcard eingesteckt wird** abgemeldet.



Um diese Funktion nutzen zu können, muss der Kartenleser, den SafeGuard PrivateDisk benutzen soll, angegeben werden. Wählen Sie den entsprechenden Kartenleser aus der Liste auf der Seite *Smartcard* aus.

3.6.4 Die Seite LDAP



Dieser Dialog steht nur in der Enterprise Edition zur Verfügung.

SafeGuard PrivateDisk erlaubt es, beim Zuweisen von Zertifikaten an ein PrivateDisk-Laufwerk über eine LDAP-Suche nach bestimmten Benutzern zu suchen.

Die Einstellungen für diese Suche werden in diesem Dialog angezeigt. Sie können hier in der Regel nicht verändert werden, da sie in der zentralen Administration über eine Administrative Vorlage festgelegt werden. Die Optionen in diesem Dialog können nur verändert werden, wenn ein Benutzer mit Administratorrechten an SafeGuard PrivateDisk angemeldet ist.

Die Suche nach bestimmten Zertifikaten (z. B. anhand der im Zertifikat enthaltenen E-Mail Adresse) ermöglicht es zum Beispiel, dem Benutzer dieses Zertifikats Zugriff auf ein PrivateDisk-Laufwerk zu gewähren, indem dem Laufwerk sein Zertifikat zugewiesen wird.

Beim eigentlichen Zuweisen des Zertifikats können diese Einstellungen lokal, auch ohne Administratorrechte verändert werden.

3.7 Passwörter und Zertifikate

Ein PrivateDisk-Laufwerk kann genau ein Administrator-Passwort und ein Benutzer-Passwort (entweder mit Lese- und Schreibrechten, oder nur mit Leserechten) haben.

Zusätzlich können einem PrivateDisk-Laufwerk Zertifikate zugeordnet werden.

Während einem PrivateDisk-Laufwerk nur zwei Passwörter zugeordnet werden können, können bis zu 32 Zertifikate zugewiesen werden.

Analog zu Passwörtern können Zertifikate mit Administratorrechten bzw. Benutzerrechten (Lesen/Schreiben oder nur Lesen) ausgestattet sein.

3.7.1 Zugriff auf PrivateDisk-Laufwerke

Anmeldung mit Passwörtern

Der Zugriff auf ein PrivateDisk-Laufwerk kann durch ein Passwort erlaubt werden. Für jedes Laufwerk bietet SafeGuard PrivateDisk drei Arten von Passwörtern. Es kann jedoch zusätzlich zum Administrator-Passwort nur ein weiteres Benutzer-Passwort vergeben werden.

- **Administrator-Passwort:**

Ist das initiale Passwort für jedes neue PrivateDisk-Laufwerk. Unter Verwendung des Master-Passworts kann ein zusätzliches Benutzer-Passwort vergeben werden, das Benutzer-Passwort kann zurückgesetzt werden (auch wenn es nicht bekannt ist), das Administrator-Passwort selbst kann geändert werden und zusätzlich können der PrivateDisk Zertifikate zugewiesen werden.

Hinweis: Es können auch Zertifikate mit Administratorrechten verwendet werden. Beim Anlegen eines neuen virtuellen Laufwerks kann auch ein Zertifikat für diese Administrationsaufgaben spezifiziert werden.

- **Benutzer-Passwort mit Lese- und Schreibrechten:**

Dieses Passwort erlaubt es dem Benutzer, sich an ein PrivateDisk-Laufwerk anzumelden und auf die darin gespeicherten Daten zuzugreifen.

- **Benutzer-Passwort mit Leserechten:**

Dieses Passwort erlaubt es dem Benutzer, sich an ein PrivateDisk-Laufwerk anzumelden, er kann jedoch den Inhalt des Laufwerks nur lesen.

Anmeldung mit Zertifikaten

Die Verwendung von Passwörtern für PrivateDisk-Laufwerke ist optional. Zertifikate können anstelle von oder zusätzlich zu Passwörtern verwendet werden.

Bis zu 32 Zertifikate können einem PrivateDisk-Laufwerk zugeordnet werden. In diesem Fall wird der öffentliche Schlüssel aus dem Zertifikat zur Verschlüsselung des Disk Encryption Keys verwendet. Nur der Besitzer des Zertifikats hat Zugriff auf den zum Zertifikat gehörenden privaten Schlüssel und kann es zur Anmeldung an das PrivateDisk-Laufwerk benutzen.

Analog zu Passwörtern können Zertifikate mit Administratorrechten bzw. Benutzerrechten (Lesen/Schreiben oder nur Lesen) ausgestattet sein.

Die Anmeldung an PrivateDisk-Laufwerke mit Zertifikaten hat einige Vorteile:

- Administratoren können Benutzern sehr einfach Benutzerrechte für ein PrivateDisk-Laufwerk geben, indem sie den öffentlich verfügbaren Teil des Zertifikats verwenden.
- Es besteht keine Notwendigkeit, initiale Passwörter zu erzeugen und zu verteilen.
- Wie Passwörter können Zertifikate entweder mit Benutzerrechten (können Daten entweder nur lesen, oder lesen und schreiben) oder Administratorrechten (können Passwörter und zugewiesene Zertifikate ändern) ausgestattet sein.
- Um Zertifikate einem PrivateDisk-Laufwerk hinzuzufügen bzw. diese zu entfernen, muss sich ein Benutzer zuerst als Administrator authentisieren (entweder durch die Verwendung eines Administrator-Passworts oder durch den Besitz eines Zertifikats mit Administratorrechten).

Master-Passwort

Werden mehrere PrivateDisk-Laufwerke verwendet, muss sich der Benutzer alle Passwörter merken und bei der Anmeldung eingeben, was unbequem ist und den Benutzer verleiten kann, dasselbe Passwort für alle seine PrivateDisk-Laufwerke zu verwenden. Dies wiederum stellt ein Sicherheitsrisiko dar.

Für solche Fälle stellt SafeGuard PrivateDisk die Funktionalität eines Master-Passworts zur Verfügung, bei der sich SafeGuard PrivateDisk für den Benutzer die verschiedenen Passwörter „merkt“. Die Passwörter werden verschlüsselt in der Windows Registrierung gespeichert und werden automatisch verwendet, wenn der Benutzer versucht, sich an ein PrivateDisk-Laufwerk anzumelden. Zur Sicherung der Passwortliste wird ein Master-Passwort verwendet. Der Benutzer muss sich dann nur dieses eine Master-Passwort merken.

Automatische Anmeldung

SafeGuard PrivateDisk kann so konfiguriert werden, dass der Benutzer automatisch an PrivateDisk-Laufwerke angemeldet wird, wenn er sich an das Betriebssystem anmeldet. Natürlich nach Eingabe des korrekten Passworts.

Der Benutzer wird automatisch von PrivateDisk-Laufwerken abgemeldet, wenn sich der Benutzer vom Betriebssystem abmeldet. Zusätzlich können PrivateDisk-Laufwerke automatisch nach Ablauf einer konfigurierbaren Zeitspanne ohne Zugriff geschlossen werden.

Smartcard-Unterstützung

SafeGuard PrivateDisk unterstützt die Verwendung von Zertifikaten, die auf Smartcards gespeichert sind. Bei der Anmeldung an ein PrivateDisk-Laufwerk wird der auf der Smartcard gespeicherte private Schlüssel verwendet.

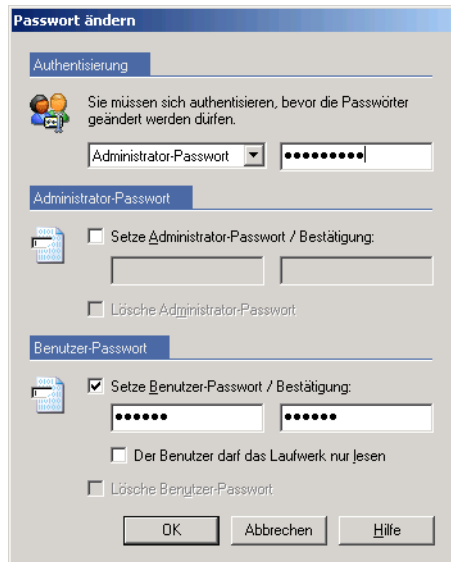
SafeGuard PrivateDisk reagiert auf das Einstecken und Ziehen der Smartcards und kann Benutzer automatisch von PrivateDisk-Laufwerken an- bzw. abmelden.

- Wird eine Smartcard in den Kartenleser eingesteckt, wird der Benutzer automatisch an SafeGuard PrivateDisk-Laufwerke mit der Start-Option **Anmelden, wenn Smartcard eingesteckt wird** angemeldet.
- Wird die Smartcard aus dem Kartenleser entfernt, wird der Benutzer von allen PrivateDisk-Laufwerken mit der Start-Option **Anmelden, wenn Smartcard eingesteckt wird** abgemeldet.

Hinweis: Die Verwaltung von Zertifikaten ist keine Aufgabe von SafeGuard PrivateDisk. Die Verwaltung der Zertifikate kann durch eine firmen-eigene PKI Infrastruktur oder von Trust Centern durchgeführt werden.

3.7.2 Passwörter bearbeiten

Zum Bearbeiten von Passwörtern stellt SafeGuard PrivateDisk den Dialog *Passwort ändern* zur Verfügung. Um diesen Dialog zu öffnen, klicken Sie auf **Passwörter** in der Symbolleiste oder klicken Sie auf **Passwort ändern...** im Menü *Bearbeiten*.



Dieser Dialog erlaubt das:

- **Setzen und Ändern des Administrator-Passworts**
Um das Administrator-Passwort ändern zu können, muss der Benutzer Administratorrechte für dieses PrivateDisk-Laufwerk haben (entweder, indem er das alte Administrator-Passwort weiß, oder indem er im Besitz eines Zertifikats mit Administratorrechten ist).
- **Setzen und Ändern des Benutzer-Passworts:**
Zum Ändern des Benutzer-Passworts muss der Benutzer in der Lage sein, sich an das PrivateDisk-Laufwerk anzumelden (entweder, indem er das alte Benutzer- oder Administrator-Passwort weiß, oder indem er im Besitz eines Zertifikates mit Administratorrechten ist).
- **Löschen des Benutzer-Passwortes:**
Um das Benutzer-Passwort löschen zu können, muss der Benutzer Administratorrechte für dieses PrivateDisk-Laufwerk haben (entweder, indem er das alte Administrator-Passwort weiß, oder indem er im Besitz eines Zertifikates mit Administratorrechten ist).

Zum **Ändern des Administrator-Passworts** müssen Sie sich mit dem Administrator-Passwort an das PrivateDisk-Laufwerk anmelden:

- Wählen Sie **Administrator-Passwort** im Abschnitt *Authentisierung des Passwort ändern* Dialoges und geben Sie das Administrator-Passwort ein.
- Aktivieren Sie die Option **Setze Administrator-Passwort**.
- Geben Sie ein neues Administrator-Passwort ein und bestätigen Sie es.

Hinweis: Wenn Sie ein Zertifikat mit Administratorrechten verwenden (durch Auswählen von **Zertifikat** im Abschnitt *Authentisierung*) können Sie auch ein Administrator-Passwort löschen, wenn Sie die entsprechende Option auswählen. Sie können das Private-Disk Laufwerk dann nur verwalten, wenn Sie den privaten Schlüssel des Zertifikats mit den Administratorrechten besitzen.

Das Setzen und Ändern von Benutzer-Passwörtern wird auf dieselbe Weise durchgeführt.

Wenn Sie sich mit dem Benutzer-Passwort an ein PrivateDisk-Laufwerk anmelden, können Sie nur das Benutzer-Passwort ändern.

Das **Setzen und Löschen** eines Benutzer-Passworts für ein PrivateDisk-Laufwerk ist nur möglich, wenn Sie sich mit Administratorrechten an das PrivateDisk-Laufwerk angemeldet haben (entweder über das Administrator-Passwort oder, indem Sie den privaten Schlüssel eines Zertifikats mit Administratorrechten besitzen).

3.7.3 Passwortverzögerung

Nach Eingabe des falschen Passworts wird ein erneuter Versuch verzögert. Diese Verzögerung erhöht sich über 2 und 5 bis auf 10 Sekunden. Der maximale Wert für die Verzögerung beträgt 20 Sekunden. Diese Verzögerung wird einzeln für die letzten zehn verwendeten PrivateDisk-Laufwerke gespeichert.

3.7.4 Zuweisen von Zertifikaten

Der Zugriff auf ein PrivateDisk-Laufwerk kann auch durch Zertifikate (bis zu 32 für ein PrivateDisk-Laufwerk) erfolgen:

Hinweis: Es ist nicht möglich, dass mehrere Benutzer mit Lese- und Schreibrechten gleichzeitig auf ein PrivateDisk-Laufwerk zugreifen. Sollen mehrere Benutzer gleichzeitig Zugriff auf ein PrivateDisk-Laufwerk haben, dürfen alle nur mit Leserechten darauf zugreifen.

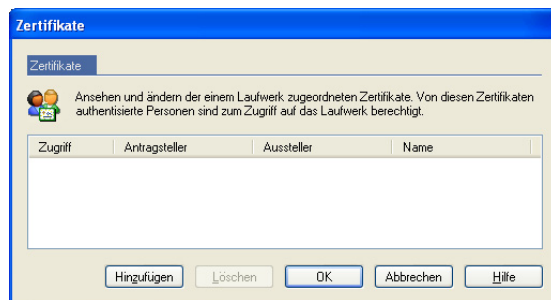
Analog zu Passwörtern unterscheidet SafeGuard PrivateDisk zwischen

- Administrator-Zertifikaten
- Benutzer-Zertifikaten
- Zertifikaten mit Leserechten

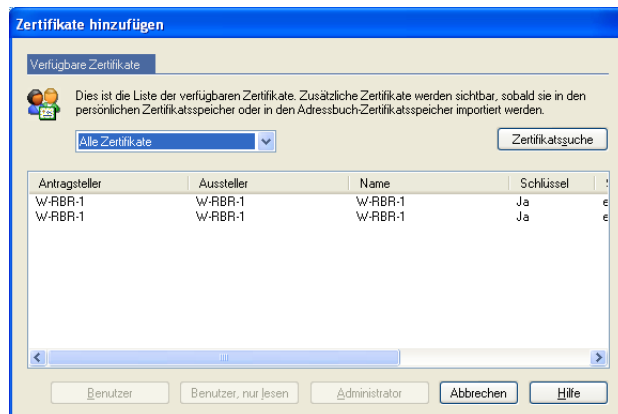
Hinweis: Um Zertifikate zuweisen zu können, müssen Sie sich mit dem Administrator-Passwort oder einem bereits zugewiesenen Administrator-Zertifikat anmelden.

Zum Zuweisen eines Zertifikats:

1. Klicken Sie auf **Zertifikate** in der Symbolleiste oder klicken Sie auf **Zertifikate...** im Menü *Bearbeiten*.
2. Geben Sie das Administrator-Passwort für die PrivateDisk ein, und klicken Sie auf OK. Der Dialog *Zertifikate* wird angezeigt.



3. Alle Zertifikate, die der PrivateDisk zugewiesen sind, werden in diesem Dialog angezeigt.
4. Zum Hinzufügen eines Zertifikats klicken Sie auf die Schaltfläche **Hinzufügen**. Der Dialog *Zertifikate hinzufügen* wird angezeigt



5. Eine Liste aller Zertifikate, die zur Verfügung stehen, wird angezeigt.

Hinweis: Nur Zertifikate, die unter Benutzerkonfiguration im Zertifikatsspeicher **Eigene Zertifikate**, **Adressbuch** und **Andere Personen** sowie unter Richtlinien für Lokaler Computer im Zertifikatsspeicher **Eigene Zertifikate** gespeichert sind, werden von SafeGuard PrivateDisk aufgelistet. Zertifikate, die an anderen Orten gespeichert sind, werden von SafeGuard PrivateDisk in dieser Liste nicht berücksichtigt.

Zertifikat über LDAP suchen

Wenn Sie ein Zertifikat zuweisen wollen, das noch nicht in diesen Zertifikatsspeichern enthalten ist, bietet SafeGuard PrivateDisk die Möglichkeit, ein Zertifikat über eine LDAP-Suche zu finden. Die Einstellungen für die LDAP-Suche können zentral definiert werden und werden auf der *Seite LDAP* unter den Optionen angezeigt.

- Um nach einem Zertifikat zu suchen, klicken Sie im Dialog *Zertifikate Hinzufügen* auf **Zertifikatssuche**. Der Dialog *LDAP Suche* wird geöffnet.
- Klicken Sie auf die Schaltfläche **Suchen**. SafeGuard PrivateDisk zeigt alle Zertifikate an, die aufgrund der angegebenen Suchdaten (Verbindungsdaten und Suchfilter) gefunden werden können.
Filter werden so definiert, dass nach bestimmten Daten im Zertifikat gesucht wird (z. B. E-Mail Adresse). Wird für die Suche nach einem bestimmten Zertifikat die E-Mail Adresse zur Identifikation verwendet, werden Sie aufgefordert, die E-Mail Adresse der Person, deren Zertifikat Sie dem PrivateDisk-Laufwerk zuweisen wollen, einzugeben.
Zur Zertifikatssuche können aber auch andere Daten verwendet werden. Entsprechend den vom Administrator definierten Filtern werden Sie aufgefordert, die notwendige Information einzugeben. Beachten Sie bitte, dass die Daten (z. B. cn - Common Name) genau so eingegeben werden müssen, wie sie im Zertifikat enthalten sind.
- SafeGuard PrivateDisk zeigt im unteren Teil des Dialogs alle Zertifikate an, die den Suchkriterien entsprechen. Es werden nur Zertifikate angezeigt, die mit SafeGuard PrivateDisk verwendet werden können.
- Durch Markieren des gewünschten Zertifikats und Klicken auf **Hinzufügen** wird das Zertifikat in die Liste der verfügbaren Zertifikate übernommen und kann nun einem Laufwerk zugeordnet werden. Der öffentliche Teil des Zertifikats wird in den Zertifikatsspeicher kopiert.

LDAP Suche bearbeiten

Durch Klicken auf die Schaltfläche **Erweitert**, werden die LDAP-Einstellungen angezeigt und können bearbeitet werden. Diese Einstellungen sollten ausschließlich von einem Administrator geändert werden, da sie umfangreiche LDAP-Kenntnisse voraussetzen.

Für einen „normalen“ Benutzer kann aber das Wechseln des verwendeten Filters von Bedeutung sein. Es können verschiedene Filter zum Beispiel für die Suche nach der E-Mail Adresse oder nach dem Common Name im Zertifikat definiert sein. Unter *Filter* können Sie einen der vordefinierten Filter auswählen. Wenn Sie die Zeile *Filter* in diesem Dialog löschen, werden alle Zertifikate, die im angegebenen LDAP-Verzeichnisdienst gefunden werden, angezeigt. Dies kann hilfreich sein, wenn Sie z. B. die genaue Schreibweise der gesuchten Daten (Benutzername im Zertifikat, Common Name, E-Mail Adresse, ...) nicht wissen. Sie können dann in der Liste der Zertifikate nach dem gewünschten suchen. Beachten Sie bitte, dass Sie bei diesem Vorgehen u. U. sehr lange Listen von Zertifikaten erhalten!

Einstellungen speichern

Wenn Sie die Einstellungen im Dialog *LDAP Suche* ändern, können Sie diese mit den beiden Schaltflächen, die sich oben rechts befinden speichern und wieder laden. Beim Speichern der Einstellungen müssen Sie einen Namen für diese Einstellungen vergeben. Durch diesen Namen können Sie die Einstellungen später wieder identifizieren. Beim Laden können Sie die gewünschten Einstellungen aus einer Liste auswählen.

6. Wählen Sie aus der Liste ein Zertifikat aus und klicken Sie abhängig davon, welche Rechte Sie dem Benutzer geben wollen, auf:

- Benutzer
- Benutzer, nur lesen
- Administrator

7. Das Zertifikat wird nun in der Liste der Zertifikate, die der PrivateDisk zugeordnet sind, angezeigt.

Unter *Zugriff* werden die jeweiligen Rechte, die mit diesem Zertifikat verknüpft sind, angezeigt.

3.7.5 Entfernen von Zertifikaten

Zum Entfernen eines Zertifikats:

1. Klicken Sie auf **Zertifikate** in der Symbolleiste oder klicken Sie auf **Zertifikate...** im Menü *Bearbeiten*.
2. Geben Sie das Administrator-Passwort für die PrivateDisk ein, oder verwenden Sie Ihr Zertifikat zur Authentisierung und klicken Sie auf **OK**. Der Dialog *Zertifikate* wird angezeigt.
3. Markieren Sie das gewünschte Zertifikat und klicken Sie anschließend auf **Löschen**. Der Besitzer des zum Zertifikat gehörenden privaten Schlüssels hat keinen Zugriff auf die PrivateDisk mehr.

3.8 SafeGuard Enterprise Schlüssel

Für die Anmeldung an ein PrivateDisk-Laufwerk können SafeGuard Enterprise Schlüssel verwendet werden. Ist ein Schlüsselring vorhanden, werden die SafeGuard Enterprise Schlüssel beim Erstellen des Laufwerks mit dem SafeGuard PrivateDisk Assistenten zur Auswahl angeboten.

Wird dem Laufwerk ein SafeGuard Enterprise Schlüssel zugewiesen, wird ausschließlich dieser Schlüssel für die Anmeldung an das PrivateDisk-Laufwerk verwendet. Es ist kein zusätzliches Passwort notwendig. Ist der Schlüssel auf dem Computer vorhanden, wird er automatisch verwendet, wenn sich der Benutzer an das PrivateDisk-Laufwerk anmeldet. Ist die Option *Anmelden, wenn sich der Benutzer ans System anmeldet* für das Laufwerk aktiviert, erfolgt die Anmeldung vollständig transparent. Das Laufwerk steht nach der Anmeldung an Windows zur Verfügung.

Lokale Schlüssel

SafeGuard Enterprise unterscheidet zwischen zentral erstellten und automatisch an die Benutzer verteilten und auf den Client-Computern lokal erzeugten Schlüsseln. Lokale Schlüssel verfügen über eine Passphrase, die den Zugriff auf diese Schlüssel ermöglicht.

Auch lokal erzeugte Schlüssel können zur Anmeldung an PrivateDisk-Laufwerke verwendet werden. Ist der Schlüssel auf dem Computer vorhanden, wird er ebenfalls automatisch zur Anmeldung verwendet.

Ist der lokale Schlüssel auf dem Computer nicht vorhanden, wird der Benutzer bei der Anmeldung aufgefordert, die Passphrase einzugeben.

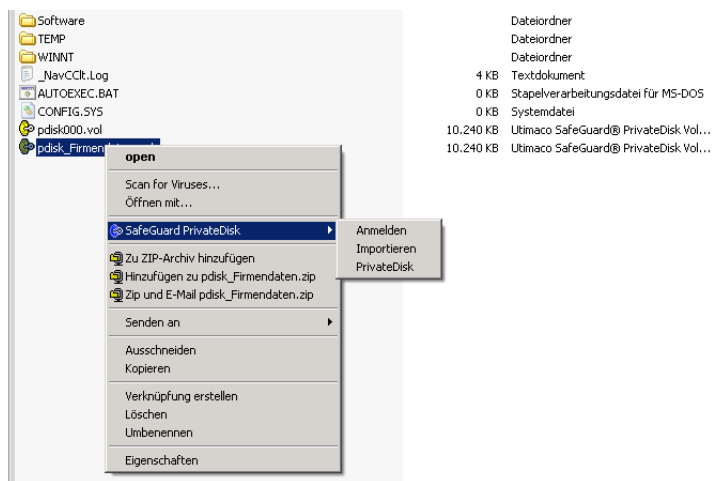
Soll einem Benutzer, der den lokalen Schlüssel eines PrivateDisk-Laufwerks nicht besitzt, Zugriff auf dieses Laufwerk gegeben werden, muss ihm die Passphrase des Schlüssels bekanntgegeben werden.

3.9 Windows Explorer-Erweiterungen

SafeGuard PrivateDisk erweitert das Windows Explorer-Kontextmenü um einen SafeGuard PrivateDisk-Eintrag.

Abhängig davon, welche PrivateDisk-Datei oder welches PrivateDisk-Laufwerk im Explorer ausgewählt wird, stehen folgende Kommandos zur Verfügung:

- Wenn Sie mit der rechten Maustaste auf eine PrivateDisk-Datei (.vol) klicken, wird ein Kommando zum Anmelden bzw. Abmelden (abhängig vom aktuellen Status) und zum Starten der Benutzeranwendung angezeigt.
- Wenn Sie mit der rechten Maustaste auf eine PrivateDisk-Datei (.vol) klicken, die noch nicht in die Liste der verfügbaren PrivateDisk-Laufwerke in der Benutzeranwendung aufgenommen wurde, ist zusätzlich ein **Importieren** Kommando verfügbar. Klicken auf **Importieren** fügt die PrivateDisk-Datei der Liste verfügbarer Laufwerke in der SafeGuard PrivateDisk-Benutzeranwendung hinzu.



4 SafeGuard PrivateDisk Portable

SafeGuard PrivateDisk Portable ermöglicht den Zugriff auf PrivateDisk-Laufwerke auch wenn SafeGuard PrivateDisk selbst nicht auf dem Computer installiert ist.

Dies wird durch ein eigenes Programm (PDPortable.exe) erreicht, das auf ein Wechselmedium kopiert wird. SafeGuard PrivateDisk Portable wird beim Erzeugen eines Private-Disk Laufwerkes auf einem Wechselmedium durch Auswählen einer entsprechenden Option auf das Wechselmedium kopiert.

Wird das Wechselmedium mit einem Computer ohne SafeGuard PrivateDisk verbunden, besteht zunächst keine Möglichkeit auf das PrivateDisk-Laufwerk zuzugreifen. Wird SafeGuard PrivateDisk Portable gestartet, kann das PrivateDisk Laufwerk ausgewählt werden und nach Eingabe des Kennwortes für das Laufwerk erhält der Benutzer lesenden Zugriff auf die verschlüsselten Dateien.

Mit SafeGuard PrivateDisk Portable können dem PrivateDisk-Laufwerk keine Dateien hinzugefügt werden. Es können aber Dateien aus dem PrivateDisk-Laufwerk an einem anderen Ort abgespeichert werden. Diese Dateien werden dort unverschlüsselt gespeichert.

4.1 PrivateDisk-Laufwerke öffnen

So öffnen Sie eine PrivateDisk-Laufwerk:

1. Starten Sie SafeGuard PrivateDisk Portable mit einem Doppelklick auf `PDPortable.exe`.
2. Klicken Sie auf **Datei > Öffnen** und wählen Sie das PrivateDisk-Laufwerk aus.
3. Geben Sie das Kennwort für das PrivateDisk-Laufwerk ein.

Hinweis: Sollen verschlüsselte Daten auf diese Weise ausgetauscht werden, muss dem Empfänger das Kennwort des PrivateDisk-Laufwerkes mitgeteilt werden.

4. SafeGuard PrivateDisk Portable zeigt jetzt das Laufwerk und seinen Inhalt an. Es steht Ihnen eine ähnliche Funktionalität, wie Sie sie vom Windows Explorer kennen, zur Verfügung.
5. Sie können Dateien durch einen einen Doppelklick öffnen.

4.2 Dateien extrahieren

So extrahieren Sie Dateien aus einem PrivateDisk-Laufwerk:

1. Wählen Sie die Datei/ die Dateien aus.
2. Klicken Sie auf **Bearbeiten** > **Extrahieren**.
3. Wählen Sie einen Speicherort für die Datei/ die Dateien aus.
4. Klicken Sie auf **Speichern**.

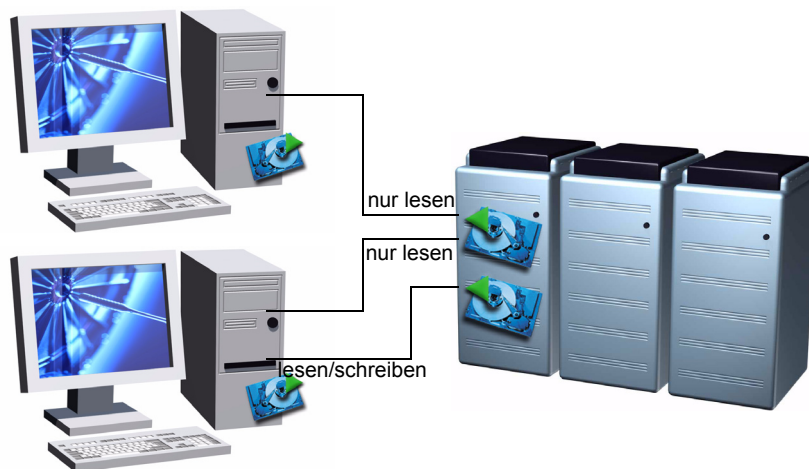
5 Anwendungsbeispiele

SafeGuard PrivateDisk ist eine benutzerfreundliche Lösung zum Sichern von Daten auf Arbeitsstationen, Notebooks, File Servern und Terminal Servern. Die folgenden Beispiele zeigen einige typische Szenarien, wie vertrauliche Daten mit SafeGuard PrivateDisk geschützt werden können.

5.1 PC-Arbeitsplatz

Anwender an einem PC-Arbeitsplatz legen PrivateDisk-Laufwerke üblicherweise auf lokalen Festplatten oder auf Netzwerk-Laufwerken an. SafeGuard PrivateDisk garantiert die Vertraulichkeit der Daten, auch wenn sie über das Netzwerk ausgetauscht werden. Dazu muss ein Benutzer sich nur an das PrivateDisk-Laufwerk auf dem Server anmelden. SafeGuard PrivateDisk muss nur auf dem Arbeitsplatz-Rechner installiert werden. Es ist nicht notwendig, SafeGuard PrivateDisk auf dem Server zu installieren. Auf dem Server wird das PrivateDisk-Laufwerk nur gespeichert.

Das Beispiel zeigt ein einfaches Netzwerk bestehend aus zwei Arbeitsplatzrechnern und einem Server. Eines der beiden PrivateDisk-Laufwerke wird von beiden Arbeitsplatz-Rechner verwendet. Aus diesem Grund wird von beiden Rechner aus darauf nur mit Leserechten zugegriffen. Auf das zweite PrivateDisk-Laufwerk auf dem Server wird nur von einem Arbeitsplatz-Rechner aus zugegriffen. Darum kann von hier aus mit Lese- und Schreibrechten zugegriffen werden.



Vorteile durch die Verwendung von SafeGuard PrivateDisk:

- Benutzer können vertrauliche Daten sicher auf Servern speichern.
- Benutzer können gleichzeitig mit Leserechten auf das PrivateDisk-Laufwerk zugreifen.

- Daten, die zwischen dem Arbeitsplatz-Rechner und dem Server ausgetauscht werden, bleiben immer verschlüsselt, da die Ver- und Entschlüsselung auf dem Arbeitsplatz-Rechner durchgeführt wird.
- Auf dem Server wird keine zusätzliche Rechenleistung benötigt, da die Verschlüsselung auf den Arbeitsplatz-Rechnern durchgeführt wird.
- Systemadministratoren haben keinen Zugriff auf die vertraulichen Daten, wenn sie nicht autorisiert sind, sich an den PrivateDisk-Laufwerken anzumelden. Dies erlaubt zum Beispiel eine Trennung zwischen Systemadministrator und Sicherheitsadministrator.
- Zentral gespeicherte PrivateDisk-Laufwerke können von einem Sicherheitsadministrator angelegt werden.
- PrivateDisk-Dateien (.vol) auf Servern können einfach in den Back-Up-Plan eines Unternehmens eingebunden werden.

Hinweis: Da der Zugriff auf ein PrivateDisk-Laufwerk wie der Zugriff auf eine einzelne Datei behandelt wird, können nicht mehrere Benutzer gleichzeitig auf ein PrivateDisk-Laufwerk mit Lese- und Schreibrechten zugreifen.

Gleichzeitiger Lese- und Schreibzugriff auf PrivateDisk-Laufwerke

PrivateDisk-Laufwerke können im Netzwerk freigegeben werden wie „normale“ Laufwerke. Wird SafeGuard PrivateDisk auf einem Server installiert, kann auf diesem Server ein PrivateDisk-Laufwerk für die Benutzer im Netzwerk freigegeben werden. Die Arbeitsplatz-Rechner können diese freigegebenen PrivateDisk-Laufwerke verbinden, wie Standard-Netzwerkordner. Benutzergruppen können dann vollen Zugriff (Lese- und Schreibrechte) auf dieses freigegebene PrivateDisk-Laufwerk haben.

Bitte beachten Sie:

- Der Zugriff auf das PrivateDisk-Laufwerk wird dann nur durch das Betriebssystem geschützt (durch Passwörter oder Benutzerrechte). Benutzer müssen sich nicht mehr an der PrivateDisk anmelden.
- Die Daten werden unverschlüsselt zwischen Arbeitsplatz-Rechner und Server übertragen, da die Verschlüsselung auf dem Server stattfindet.
- Die Anmeldung an das PrivateDisk-Laufwerk (das „Öffnen“ des Laufwerks) muss auf dem Server von einer autorisierten Person durchgeführt werden.

5.2 Mobile Benutzer

Das größte Sicherheitsrisiko, das Notebookanwendern droht, ist Diebstahl. SafeGuard PrivateDisk kann zwar den Diebstahl eines Notebooks nicht vereiteln, aber es verhindert, dass vertrauliche Daten von Unbefugten gelesen werden können.

Das Beispiel zeigt ein Notebook mit einem lokalen PrivateDisk-Laufwerk und einem zweiten PrivateDisk-Laufwerk auf CD-ROM (z. B. mit internen Produktinformationen und Preislisten). So können beispielsweise Updates zwischen der Zentrale und dem mobilen Nutzer durch PrivateDisk-Dateien (.vol) auf CD-ROMs gesichert werden. Nur berechtigte Anwender (durch das Passwort oder indem sie den zum Zertifikat gehörenden privaten Schlüssel besitzen) können das PrivateDisk-Laufwerk öffnen und den Inhalt lesen.



Vorteile durch die Verwendung von SafeGuard PrivateDisk:

- Vertrauliche Daten sind auf der lokalen Festplatte geschützt, sowohl wenn der Rechner eingeschaltet ist, als auch wenn er verloren geht oder gestohlen wird.
- Für unbefugte Personen sieht die Virtual Disk wie eine einfache Datei aus und die Ordnerstruktur bleibt ihnen verborgen.
Die Daten bleiben auch vor Personen mit physischen Zugriff auf den Rechner geschützt solange das Passwort, das notwendig ist, um sich an das PrivateDisk-Laufwerk anzumelden, ein Geheimnis bleibt oder der zum Zertifikat gehörende private Schlüssel sicher verwahrt ist (auf Smartcard und/oder ebenfalls durch ein Passwort geschützt).
- Vertrauliche Daten können gesichert werden, ohne dass eine ganze Festplatte oder Partition verschlüsselt werden muss.
- PrivateDisk-Dateien (.vol) für PrivateDisk-Laufwerke können auf Festplatten, Netzwerklaufräumen sowie auf tragbaren Medien (Diskette, ZIP, CD-ROMs, DVD, USB- und Flash-Speicherkarten, etc.) abgespeichert werden. So können Daten auf diesen Geräten/ Medien sehr komfortabel und zuverlässig gespeichert werden.
- PrivateDisk-Dateien (.vol) können sicher über ungesicherte Kanäle wie E-Mail ausgetauscht werden.

5.3 Terminal Server

SafeGuard PrivateDisk kann auch auf einem Terminal Server installiert werden. Vertraulichkeit unter den Benutzern des Terminal Servers wird dadurch gewährleistet, dass ein PrivateDisk-Laufwerk nur für jenen Benutzer sichtbar ist, der sich daran angemeldet hat.

Vorteile durch die Verwendung von SafeGuard PrivateDisk:

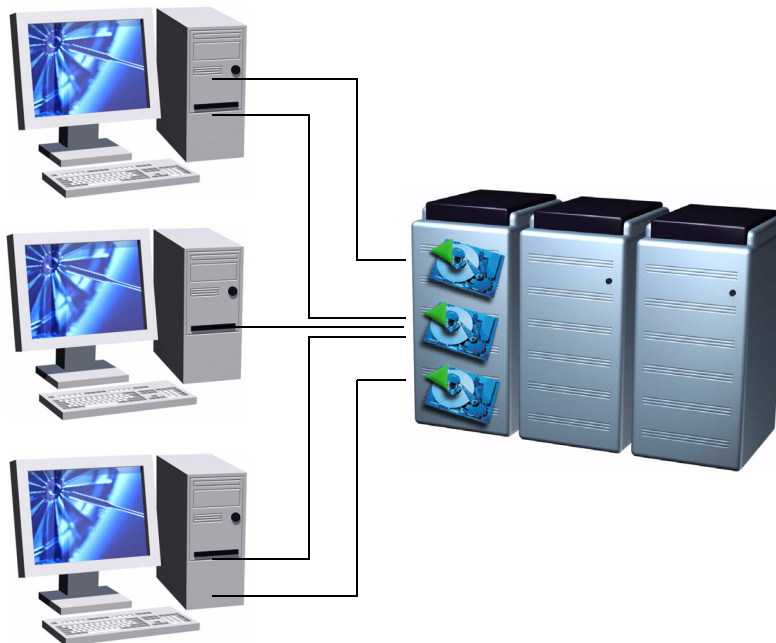
- Die Benutzer können mit vertraulichen Daten arbeiten und der Administrator des Terminal Servers hat keinen Zugriff auf diese Daten.
- PrivateDisk-Laufwerke sind nur für autorisierte Benutzer sichtbar. Meldet sich ein Benutzer an ein PrivateDisk-Laufwerk an, so ist dieses nur für jene Benutzer sichtbar, die sich ebenfalls an dieses Laufwerk angemeldet haben.

Beispiel:

Benutzer 1 öffnet ein PrivateDisk-Laufwerk als Laufwerk X.

Benutzer 2 kann Laufwerk X von Benutzer 1 nicht sehen, könnte dasselbe Laufwerk jedoch öffnen. Er könnte sogar ein anderes PrivateDisk-Laufwerk als Laufwerk X öffnen.

- Mehrere Benutzer können gleichzeitig mit Lese- und Schreibrechten auf ein einziges PrivateDisk-Laufwerk zugreifen. Dies erlaubt es Benutzergruppen, gleichzeitig mit einem einzigen PrivateDisk-Laufwerk zu arbeiten.
- Es müssen nur die Terminal Server administriert werden (Software Installation, etc.).



Die Abbildung zeigt eine Terminal Server Umgebung, in der zwei der drei Benutzer PrivateDisk-Laufwerke haben und alle Benutzer ein weiteres PrivateDisk-Laufwerk gemeinsam benutzen.

Hinweis: Obwohl mehrere Terminal Server Benutzer u. U. gleichzeitig ein PrivateDisk-Laufwerk benutzen, kann das Laufwerk, je nach Client- oder Session-Konfiguration, unterschiedliche Laufwerksbuchstaben für jede Terminal Server Session haben. So kann z. B. das gemeinsam benutzte PrivateDisk-Laufwerk im Beispiel auf dem ersten Computer das Laufwerk D und auf dem zweiten das Laufwerk E sein.

5.4 Verschlüsselte Back-Ups

SafeGuard PrivateDisk kann auch zur Erzeugung verschlüsselter Back-Ups verwendet werden.

Dazu müssen die jeweiligen Dateien nur in ein PrivateDisk-Laufwerk kopiert werden, und die PrivateDisk-Datei (.vol) muss anschließend auf das Back-Up-Medium kopiert werden.

Liegt eine PrivateDisk-Datei (.vol) eines PrivateDisk-Laufwerks auf einem Netzwerklaufwerk, so wird beim Back-Up des Netzwerkservers automatisch auch der verschlüsselte Inhalt des PrivateDisk-Laufwerks gesichert.

Vorteile durch die Verwendung von SafeGuard PrivateDisk:

- Vertrauliche Daten bleiben vor unbefugtem Zugriff auf dem Back-Up-Medium geschützt.
- Der Back-Up-Administrator hat keinen Zugriff auf vertrauliche Daten.

5.5 Fast User Switching

SafeGuard PrivateDisk unterstützt die "Fast User Switching"-Funktionalität von Windows XP. Die Integration von Terminal Server-Technologie in das Microsoft Betriebssystem bietet Anwendern eine verbesserte Flexibilität bei der gemeinsamen Nutzung von Rechnern und Dateien.

Vorteile durch die Verwendung von SafeGuard PrivateDisk:

- PrivateDisk-Laufwerke sind nur für befugte Anwender sichtbar und nutzbar. Wenn sich ein Benutzer zum Beispiel an ein PrivateDisk-Laufwerk anmeldet, ist dieses für andere Benutzer nicht sichtbar.
- Das PrivateDisk-Laufwerk eines Anwenders bleibt offen, wenn zu einem anderen Anwender gewechselt wird (Fast User Switching).
Auch auf einem gemeinsam genutzten Computer kann ein geöffnetes PrivateDisk-Laufwerk nicht von einem unbefugten Anwender eingesehen werden. So können sich mehrere Anwender einen Rechner teilen, wobei der Computer im Hintergrund Prozesse eines Anwenders bearbeiten kann, während ein anderer Anwender den Rechner für seine Applikation nutzt.

6 Zentrale Administration

6.1 Produktkonfiguration und Policy

Die Enterprise Edition von SafeGuard PrivateDisk wird mit einer administrativen Vorlage (sguard.adm) geliefert, die zum Erzeugen von Richtlinien-Dateien (wenn kein Active Directory vorhanden ist) oder Gruppenrichtlinienobjekten (für Active Directory) verwendet werden kann. Die administrative Vorlage befindet sich im Unterverzeichnis ADM des Installationsverzeichnis von SafeGuard PrivateDisk. Die administrative Vorlage enthält Einstellungen für alle Programmoptionen von SafeGuard PrivateDisk. Zusätzlich erlaubt die Vorlage Listen von PrivateDisk-Laufwerken zu erzeugen, die für den Benutzer zur Verfügung stehen sollen und die Definition eines initialen Laufwerks, das automatisch erzeugt wird, wenn der Benutzer sich an das System anmeldet.

Richtlinien die von einem Systemadministrator erzeugt werden, werden automatisch an die Arbeitsstationen verteilt, wenn sich der Benutzer an den Domänen-Server oder Active Directory anmeldet.

Da die Benutzer in einer IT-Umgebung gewöhnlich keine Administratorrechte haben, können sie selbst diese Programmeinstellungen nicht ändern.

6.1.1 Administrative Vorlage sguard.adm

Um die administrative Vorlage von SafeGuard PrivateDisk verwenden zu können, müssen Sie den Gruppenrichtlinien-Editor öffnen und die administrative Vorlage hinzufügen.

Danach wird ein *SafeGuard...* Knoten unter *Richtlinien für Lokaler Computer* und *Benutzerkonfiguration* angezeigt.

Unter *Richtlinien für Lokaler Computer* enthält die administrative Vorlage, mit Ausnahme der Passwortrestriktionen und der Zertifikatsprüfung, dieselben Einstellungen wie der Optionendialog von SafeGuard PrivateDisk.

Hinweis: Für Einstellungen die in diesem Kapitel nicht ausführlich beschrieben sind, finden Sie eine Erklärung im entsprechenden Eigenschaften Dialog der administrativen Vorlage.

System Policy Editor:

```
SafeGuard PrivateDisk
```

Group Policy Editor (Active Directory)

```
Computerkonfiguration\  
Administrative Templates\  
SafeGuard\  
PrivateDisk
```

- **Allgemein**

- **Automatisches Aktivieren von virtuellen Laufwerken**
- **Automatisches Deaktivieren von unbenutzten Laufwerken**
- **Bevorzugter CSP**

Wenn Sie Zertifikate zur Authentisierung verwenden, können Sie hier den “Cryptographic Service Provider“ (CSP) definieren, den Ihre Benutzer vorzugsweise verwenden sollen. Dies kann beispielsweise ein bestimmter Smartcard CSP sein. Der Name muss Teil des CSP-Namen aus der Registrierung sein. Der lesbare Name wird für Meldungen an den Benutzer verwendet und ist optional.

- **Anmeldung**

- **Gemeinsame Anmeldung**

- **Smartcard**

- **Kartenleser**

Achtung, beim Namen des Kartenlesers wird zwischen Groß- und Kleinschreibung unterschieden!

- **LDAP**

Unter diesem Knoten können Einstellungen festgelegt werden, die bei der Suche nach einem Zertifikat über LDAP verwendet werden. Diese Einstellungen werden auf der Seite LDAP im Optionen Dialog und beim Starten der Suche beim Zuweisen eines Zertifikats angezeigt. Im Optionen Dialog können diese Einstellungen nicht geändert werden (außer der Benutzer ist mit Administratorrechten angemeldet) beim Zuweisen des Zertifikates hingegen schon.

- **Host**

Unter Host muss der Domänenname bzw. die IP-Adresse des LDAP-Servers eingetragen werden.

- **Port**

Hier muss der TCP-Port, über den die Verbindung aufgebaut werden soll, eingetragen werden. Wird das Feld leer gelassen, so wird standardmäßig Port 389 verwendet.

- **Protokoll Version**

Hier muss die Version des zu verwendenden Protokolls aus der Liste ausgewählt werden. Standardmäßig wird Version 3. verwendet.

- **Anonym**

Ist diese Option aktiviert, wird versucht, eine anonyme Verbindung zum Host herzustellen. Soll die Verbindung nicht anonym aufgebaut werden, muss der Benutzer beim Aufbau der Verbindung gültige Zugangsdaten für den LDAP-Server eingeben.

- **Authentisierung**

Hier kann die Art der verlangten Authentisierung gegenüber dem LDAP-Server angegeben werden. Standardmäßig wird GSS (Generic Security Services) verwendet.

Die folgenden Parameter beziehen sich auf die Suche in der LDAP Struktur.

- **Basis**

Hier kann angegeben werden, ab welchem Knoten in der LDAP Struktur nach dem Zertifikat gesucht wird. Damit ist es möglich, die Suche auf einen Teilbaum einzuschränken, wodurch die Zertifikate schneller gefunden werden können (Beispiel: Suche nur in einer bestimmten OU).

Der Knoten, bei dem mit der Suche begonnen werden soll muss angegeben werden.

- **Filter**

Im Eingabefeld Filterliste kann ein Filter für die Suche nach einem Zertifikat definiert werden. Dem Benutzer werden bei der Zuweisung des Zertifikats nur Zertifikate angezeigt, die dem Filter entsprechen. So kann z. B. gezielt nach dem Common Name oder der E-Mail Adresse im Zertifikat gesucht werden.

Filtersyntax:

Ein Filter besteht aus einer Bezeichnung (Filtername), der eigentlichen Filterdefinition (der Angabe, wonach gesucht werden soll, z. B. "cn=") und optional aus einer Parameterliste. Für den variablen Teil der Filterdefinition ist "%s" einzufügen (z. B. "cn=%s"). Der Parameter (%s) wird vor der Suche abgefragt. Der Benutzer wird aufgefordert, die entsprechende Information einzugeben. Im Filter wird der Parameter durch die Benutzereingabe ersetzt.

Für jeden Platzhalter in der Filterdefinition kann in der Parameterliste ein Parametername angegeben werden. Der Parametername wird dem Benutzer bei der Eingabeaufforderung angezeigt, damit klar ist, welcher Art die geforderte Information ist.

Mehrere Parameternamen sind durch ein Komma zu trennen.

Filtername, Filterdefinition und Parameterliste sind in Hochkomma zu setzen und durch ein Komma getrennt.

Mehrere Filter sind mit einem Strichpunkt zu trennen.

Der zu verwendende Filter kann beim Zuweisen eines Zertifikats aus einer Liste von Filternamen ausgewählt werden.

Beispiel:

“Emailsuche“, “mail=%s“, “E-Mail Adresse“

Wird der Filter “Emailsuche“ bei der Suche eines Zertifikats ausgewählt, wird der Benutzer aufgefordert, die E-Mail Adresse des gesuchten Benutzers einzugeben (E-Mail Adresse wird im Dialog angezeigt). Es werden alle Zertifikate, die die entsprechende E-Mail Adresse enthalten, angezeigt.

Hinweis: Der Benutzer muss die geforderte Information genau so eingeben, wie sie im Zertifikat enthalten ist. Die E-Mail Adresse bietet sich dafür an, da sie in der Regel bekannt ist und vom Benutzer verwendet wird. Wird hingegen z. B. `cn=%s` verwendet muss der Benutzer genau wissen, wie der Common Name im Zertifikat angegeben ist.

- **Attribut**
Hier muss das Attribut angegeben werden, unter dem im Verzeichnisdienst die Zertifikate der Benutzer gespeichert sind. In der Regel ist dies das LDAP-Attribut `usercertificates`.
Standardwert ist `usercertificates`. Es darf nur ein Attribut angegeben werden.
- **Zeitlimit**
Zeitlimit für die Suche in Sekunden. Ein Wert von 0 bedeutet "kein Limit".
Zum Beispiel 30.
- **Mengenlimit**
Maximale Anzahl der gefundenen Zertifikate, die angezeigt und damit zugewiesen werden können. Ein Wert von 0 bedeutet "kein Limit". Zum Beispiel: 10
- **Passwort Restriktionen**
 - **Minimale Länge**
Hier können Sie die Mindestlänge von Passwörtern für neu angelegte PrivateDisk-Laufwerke bestimmen.
Passwörter können aus bis zu 32 Zeichen bestehen. Der Standardwert sind vier Zeichen.
- **Zertifikatsprüfung:**
 - **CRL-Überprüfung**
Wird diese Option aktiviert, werden Zertifikate nur akzeptiert, wenn sie vollständig überprüft werden können. Bitte beachten Sie, dass dies bedeutet, dass bei Bedarf eine CRL des Ausstellers des Zertifikats über das Netzwerk geladen wird.
 - **Erlaube Zertifikate mit unbekanntem kritischen Erweiterungen**
Wird diese Option aktiviert, werden die kritischen Zertifikatserweiterungen nicht überprüft. Zertifikate mit unbekanntem kritischen Erweiterungen können jetzt zugewiesen werden.
 - **Erlaube Signatur-Zertifikate**
Wird diese Option aktiviert, können reine Signatur-Zertifikate zugewiesen werden.

Unter Benutzerkonfiguration stehen folgende Einstellungen zur Verfügung:

```
Benutzerkonfiguration\  
Administrative Vorlagen\  
SafeGuard\  
PrivateDisk
```

- **Benutzerrechte**

- **Erstellen von Laufwerken**

Das Erstellen von PrivateDisk-Laufwerken auf einem Rechner muss dem Benutzer ausdrücklich erlaubt werden. Aktivieren Sie diese Option, um dem Benutzer zu erlauben, eigene Laufwerke zu erstellen.

- **Tray Icon**

Ist diese Option deaktiviert, wird das SafeGuard PrivateDisk Icon in der Task-Leiste nicht angezeigt.

- **Laufwerke**

- **Vorgeschriebenes Laufwerk**

PrivateDisk-Laufwerke, die einem Benutzer durch diese Einstellung zugewiesen werden, werden vorgeschriebene Laufwerke genannt. Die Einstellung für ein solches Laufwerk können vom Benutzer nicht geändert werden und es kann nicht aus der Liste der verfügbaren PrivateDisk-Laufwerke entfernt werden. Auf diese Weise kann von Systemadministratoren sichergestellt werden, dass bestimmte PrivateDisk-Laufwerke dem Benutzer immer zur Verfügung stehen.

Der Eintrag beschreibt ein Laufwerk im Format:

<Disk-Datei>|<Name>|<Laufwerksbuchstabe>|<Optionen>

Soll der nächste nicht verwendete Laufwerksbuchstabe bei der Anmeldung verwendet werden (siehe Option **Automatisch**), muss <Laufwerksbuchstabe> frei gelassen werden.

Beispiel: c:\Benutzer001.vol|Vorgeschrieben||L)

Start-Optionen (nur eine möglich):

L ... beim Benutzer-Logon aktivieren

P ... bei Verfügbarkeit der Disk-Datei aktivieren (Plug and Play)

C ... bei Verfügbarkeit einer Smartcard aktivieren

Zusätzliche Optionen:

R ... nur zum Lesen aktivieren

S ... Simuliere Festplatte (siehe Seite 19)

Beispiel:

c:\Benutzer001.vol|Vorgeschrieben|Z|LR

Die Disk-Datei `Benutzer001.vol` liegt auf Laufwerk C und wird als `Vorgeschrieben` in der Liste der verfügbaren PrivateDisk-Laufwerke angezeigt. Dem PrivateDisk-Laufwerk wird der Laufwerksbuchstabe `Z` zugewiesen. Der Benutzer wird an das PrivateDisk-Laufwerk nur mit Leserechten (R) angemeldet, wenn er sich an das Betriebssystem anmeldet (L).

Um für einen Benutzer automatisch ein PrivateDisk-Laufwerk zu erzeugen, siehe **Initiales Laufwerk**.

Hinweis: Existiert die Volume-Datei nicht, wird sie trotzdem in der Liste der verfügbaren PrivateDisk-Laufwerke angezeigt. Wird sie anschließend erzeugt, kann sie wie beabsichtigt verwendet werden.

- **Zertifikat für Wiederherstellung**

Hier können Sie die Seriennummer eines Zertifikats angeben, dem automatisch Administratorrechte für alle vom Benutzer neu angelegten PrivateDisk-Laufwerke zugewiesen werden. Das stellt sicher, dass immer eine Möglichkeit besteht, auf dieses PrivateDisk-Laufwerk zuzugreifen.

Die Seriennummer muss als Folge von Hex-Werten angegeben werden.

Hinweis: Datensicherheit ist gewährleistet, wenn der private Schlüssel des Zertifikats für die Wiederherstellung sicher verwahrt wird (z. B. in einem Safe, gespeichert auf einer Smartcard oder Diskette).

- **Initiales Laufwerk**

- **Initiales Laufwerk**

Ein initiales Laufwerk wird automatisch erzeugt, wenn sich der Benutzer an das Betriebssystem anmeldet und es nicht bereits existiert.

- **Benutzer soll Zertifikat statt Passwort verwenden**

Wird diese Option aktiviert, wird das Zertifikat des Benutzers automatisch dem neu angelegte PrivateDisk-Laufwerk zugewiesen. Standardmäßig ist diese Option deaktiviert.

Hinweis: Beim Erzeugen des PrivateDisk-Laufwerks auf dem Computer des Benutzers wird das Zertifikat nur zugewiesen, wenn der Benutzer im Besitz des zugehörigen privaten Schlüssels ist. Stehen dem Benutzer verschiedene Zertifikate zur Verfügung, wird beim Anlegen des Laufwerks ein Dialog angezeigt, in dem Benutzer ein Zertifikat auswählen kann.

- **LDAP**

- **Verwendeter Filter**

Hier kann ein Suchfilter, der dem Benutzer bei der Suche nach einem Zertifikat über LDAP zur Verfügung steht, angegeben werden. Es muss der Name des Filters, wie er unter *Computerkonfiguration* angegeben wurde, in das Eingabefeld eingetragen werden. Es darf nur ein Filter angegeben werden, der unter Computerkonfiguration definiert wurde.

7 SafeGuard PrivateDisk OLE Automation Interface

SafeGuard PrivateDisk exportiert einen OLE Automation Server (pdole.exe), der zur programmatischen Verwendung der Software von allen zu Windows Scripting kompatiblen Applikationen aus verwendet werden kann. Dies beinhaltet den Windows Scripting Host (Visual Basic Scripting, JavaScript, Perl, ...) ebenso wie MS Office Applikationen, Web-Seiten und Programmierumgebungen wie Visual Basic, Visual C++ und viele mehr.

Die exportierte COM Objektklasse heißt PrivateDisk.Application. Für die Scripting Kompatibilität exportiert sie ein IDispatch Interface mit den folgenden Eigenschaften und Kommandos.

7.1 Eigenschaften

Die Änderung der Eigenschaften eines PrivateDisk.Application Objekts beeinflusst nur spätere Operationen für dieses einzelne Objekt, verändert die Einstellungen anderer Objekte aber nicht.

NoGui	Boolean	Diese Option kann auf <i>True</i> gesetzt werden, wenn absolut keine GUI angezeigt werden soll. In diesem Fall werden weder Dialoge noch Message Boxes angezeigt. Standardmäßig wird diese Option auf <i>False</i> gesetzt, was zur Abfrage von Passwörtern führt, wenn diese nicht als Kommando-Parameter mitgegeben wurden und im Falle von Fehlern zur Anzeige von Message-Boxes mit Fehlerbeschreibungen führt. Wird die Eigenschaft "NoGui" auf <i>True</i> gesetzt, es ist aber eine Benutzereingabe notwendig (z. B. Eingabe eines Passworts), wird die gesamte Operation abgebrochen und ein entsprechender Fehlercode zurückgegeben.
-------	---------	---

7.2 Kommandos

Im Folgenden eine Liste von Kommandos, die für das PrivateDisk.Application Objekt aufgerufen werden können. Parameter in Klammern sind optional. Weiter unten finden Sie eine Beschreibung der einzelnen Parameter.

NewDisk volume, size, (path), (fileys), (admpwd), (usrpwd)	Erzeuge ein neues PrivateDisk-Laufwerk. Der Benutzer wird nach der Erzeugung automatisch angemeldet. Gibt <i>True</i> bei Erfolg zurück, sonst <i>False</i> .
--	---

MountDisk volume, (pwd), (pwdtype), (readonly)	Anmelden des Benutzers an ein PrivateDisk-Laufwerk, das durch seine Volume-Datei identifiziert wird. Das PrivateDisk-Laufwerk muss bereits in der Liste der für den Benutzer verfügbaren Laufwerke vorhanden sein. Wenn readonly auf <i>True</i> gesetzt ist, wird das Laufwerk nur für Lesezugriff angemeldet. Gibt <i>True</i> bei Erfolg zurück, sonst <i>False</i> .
ImportDisk volume, (path)	Fügt der Liste der für den Benutzer verfügbaren PrivateDisk-Laufwerke ein Laufwerk hinzu. Gibt <i>True</i> bei Erfolg zurück, sonst <i>False</i> .
UnmountDisk volume, (forced)	Meldet einen Benutzer von einem PrivateDisk-Laufwerk ab. Wird forced auf <i>True</i> gesetzt, wird das Laufwerk immer abgemeldet, auch wenn es noch von Programmen verwendet wird. Gibt <i>True</i> bei Erfolg zurück, sonst <i>False</i> .
UnmountAllDisks (forced)	Versucht, einen Benutzer von allen PrivateDisk-Laufwerken, an die er angemeldet ist, abzumelden. Wird forced auf <i>True</i> gesetzt, wird das Laufwerk immer abgemeldet, auch wenn es noch von Programmen verwendet wird. Gibt <i>True</i> bei Erfolg zurück, sonst <i>False</i> .
GetDiskInfo volume, (path), (mounted), (readonly)	Sammelt Informationen über den Status eines PrivateDisk-Laufwerks. Nur der <volume> Parameter wird als Input verwendet, alle anderen Werte sind Output-Parameter und werden von der Funktion geliefert, wenn sie angegeben sind. Gibt <i>True</i> bei Erfolg zurück, sonst <i>False</i> .
GetErrorText	Im Falle eines Fehlers kann diese Funktion aufgerufen werden, um den Grund in Klartext auszugeben.

7.2.1 Parameter

volume	PrivateDisk-Laufwerke werden durch ihre Volume-Datei (der Name der .vol Datei) identifiziert. Der symbolische Name kann für diesen Zweck nicht verwendet werden, da er nicht einmalig ist.
size	Disk-Größe in kBytes. Der Wert wird auf das nächste Vielfache von 4 kB gesetzt, was die Cluster-Größe von PrivateDisk-Laufwerken darstellt.
path	Beschreibt den Laufwerks-Buchstaben für ein PrivateDisk-Laufwerk. Geben Sie für Laufwerksbuchstaben einen String wie "X" oder "X:" an. Für den nächsten freien Laufwerksbuchstaben lassen Sie den Parameter leer.
filesystem	Gibt das Dateisystem für das PrivateDisk-Laufwerk an. Mögliche Werte sind „FAT“ und „NTFS“. Standardwert ist „FAT“.
usrpwd	Gibt das Benutzer-Passwort für ein neues PrivateDisk-Laufwerk an.
admpwd	Gibt das Administrator-Passwort für ein neues PrivateDisk-Laufwerk an. Wird es nicht angegeben, wird der Benutzer bei der Erzeugung des Laufwerks nach einem Administrator-Passwort gefragt.
pwd	Ist das Passwort für die Anmeldung an ein PrivateDisk-Laufwerk. Dies kann das Benutzer-Passwort, das Administrator-Passwort oder eine PIN für einen Cryptographic Service Provider sein (siehe unten <pwdtype> Parameter). Wird dieser Parameter leer gelassen, wird die Anmeldung mit Zertifikaten versucht. Wenn notwendig, wird der Benutzer nach einem Passwort gefragt.
pwdtype	Dieser Integer-Wert bestimmt die Methode bei der Anmeldung an ein PrivateDisk-Laufwerk. Er wird nur verwendet, wenn der <pwd> Parameter gesetzt ist: 0 (oder leer) ... der <pwd> Parameter ist das Administrator- Passwort 1 ... der <pwd> Parameter ist das Benutzer-Passwort 2 ... der <pwd> Parameter ist die PIN für eine Anmeldung mit Zertifikat ("silent" connect)
mounted	Dieser Wert wird auf <i>True</i> gesetzt, wenn ein Benutzer an das PrivateDisk-Laufwerk angemeldet ist. Sonst <i>False</i> .
readonly	Dieser Wert wird auf <i>True</i> gesetzt, wenn ein Benutzer nur mit Leserechten angemeldet ist. Sonst <i>False</i> .

7.3 Beispiel-Script

Ein Beispiel-Script (demo.vbs) steht im `SafeGuard PrivateDisk` Unterverzeichnis des Installationsverzeichnisses von SafeGuard PrivateDisk zur Verfügung.

8 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

9 Rechtliche Hinweise

Copyright © 2000 - 2011 Sophos Group Alle Rechte vorbehalten. SafeGuard ist ein eingetragenes Warenzeichen von Sophos Group.

Sophos ist ein eingetragenes Warenzeichen von Sophos Limited, Sophos Group bzw. Utimaco Safeware AG. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.