

KASPERSKY LAB

---

# **Kaspersky KryptoStorage 1.0**

**Benutzerhandbuch**

**KASPERSKY KRYPTOSTORAGE 1.0**

---

# **Benutzerhandbuch**

© Kaspersky Lab

<http://www.kaspersky.com>

Erscheinungsdatum: Januar 2010

# Inhalt

KAPITEL 1. EINFÜHRUNG IN KASPERSKY KRYPTOSTORAGE .....	5
1.1. Komponenten von Kaspersky KryptoStorage .....	7
1.2. Geschützte Objekte .....	7
1.3. Zugriffsberechtigungen auf geschützte Objekte .....	8
1.4. Empfehlungen zum Erstellen eines Kennworts und eines Kennworthinweises .....	9
KAPITEL 2. KASPERSKY KRYPTOSTORAGE INSTALLIEREN .....	11
2.1. Hardware- und Softwarevoraussetzungen .....	11
2.2. Installationsbeschreibung .....	12
2.3. Lizenzverwaltung .....	14
2.4. Lizenzschlüssel mit Aktivierungscode abrufen und installieren .....	16
2.5. Produktversion aktualisieren.....	18
KAPITEL 3. BENUTZEROBERFLÄCHE DES SYSTEMS .....	19
3.1. Kontextmenü im Explorer .....	19
3.2. Fenster der Steuerung von Kaspersky KryptoStorage.....	20
KAPITEL 4. DATENSCHUTZ DURCH DIE VERWENDUNG GESCHÜTZTER OBJEKTE           22	
4.1. Geschützte Ordner.....	22
4.1.1. Ordner erstellen .....	23
4.1.2. Regeln zur Verwendung geschützter Ordner.....	25
4.1.3. Geschützte Ordner einbinden.....	27
4.1.4. Geschützte Ordner trennen .....	27
4.2. Geschützte Container .....	28
4.2.1. Container erstellen.....	28
4.2.2. Verwendung vorbereiten .....	31
4.2.3. Regeln für die Verwendung von Containern .....	31
4.2.4. Container einbinden .....	31
4.2.5. Container formatieren.....	33
4.2.6. Container trennen.....	34
4.2.7. Löserschutz.....	35
4.3. Logische Festplattenpartitionen und Wechseldatenträger verschlüsseln.....	35

---

4.3.1. Besonderheiten bei der Verwendung von Programmen für die Arbeit mit Festplatten .....	37
4.3.2. Verschlüsseln .....	38
4.3.3. Verschlüsselungsvorgang unterbrechen .....	40
4.3.4. Verschlüsselungsvorgang fortsetzen.....	41
4.3.5. Objekt in den unverschlüsselten Zustand zurücksetzen.....	41
4.3.6. Objekt entschlüsseln .....	42
4.3.7. Bootvorgang von verschlüsseltem System- bzw. Bootlaufwerk ausführen .....	43
4.3.8. Geschützte logische Festplattenpartitionen und Wechseldatenträger einbinden.....	44
4.3.9. Geschützte logische Festplattenpartitionen und Wechseldatenträger trennen .....	44
4.3.10. Laufwerke wiederherstellen .....	45
4.4. Sicheres Löschen von geschützten und ungeschützten Objekten.....	47
KAPITEL 5. SUBSYSTEME KONFIGURIEREN.....	48
KAPITEL 6. KASPERSKY KRYPTOSTORAGE DEINSTALLIEREN.....	51
APPENDIX A. GLOSSAR .....	53
APPENDIX B. REFERENZINFORMATIONEN.....	55
B.1. Kaspersky Lab.....	55
B.2. Lizenz für die Bibliothek Windows Installer XML (WiX) .....	56

# KAPITEL 1. EINFÜHRUNG IN KASPERSKY KRYPTOSTORAGE

Kaspersky KryptoStorage (nachfolgend Kaspersky KryptoStorage oder System genannt) ist ein System für den kryptografischen Schutz vor einem unerlaubten Datenzugriff auf vertrauliche Daten, die auf einem PC gespeichert sind.

Das System ist für den Schutz vertraulicher Informationen eines Benutzers vor dem unerlaubten Datenzugriff, zur Vorbeugung vor Datendiebstahl beim Speichern von Informationen durch das Betriebssystem auf der Festplatte und vor Beschädigungen von Dateien des Benutzers konzipiert.

Für den Datenschutz wird der Mechanismus einer **transparenten Verschlüsselung** angewendet.

Bei der **transparenten Verschlüsselung** handelt es sich um einen Mechanismus, durch den Daten in einem geschützten Objekt ausschließlich in verschlüsselter Form gespeichert werden. Die Arbeit in dem geschützten Objekt erfolgt so, daß die Daten beim Zugriff darauf automatisch im Arbeitsspeicher entschlüsselt und beim Speichern wieder verschlüsselt werden.

Als Verschlüsselungsalgorithmus wird AES (Advanced Encryption Standard) mit einer Schlüssellänge von 128 Bit verwendet. Dieser Algorithmus wurde von einer internationalen kryptografischen Gemeinschaft als Standard in der Kryptografie formuliert und vom National Institute of Standards and Technology (NIST) der USA (Federal Information Processing Standards (FIPS), Veröffentlichung 197 vom 26.11.2001) öffentlich bekannt gegeben.

Der kryptografische Schlüssel wird auf Grundlage des Benutzerkennworts generiert. Im Zusammenhang damit ist zu beachten, daß die Länge des Kennworts bedingt durch die regionalen gesetzlichen Bestimmungen beschränkt sein kann.

Im Folgenden sind die Hauptfunktionen des Systems aufgeführt.

## **Datenschutz**

Das System bietet folgende Möglichkeiten:

- Erstellen einzelner geschützter Ordner im NTFS-Dateisystem zum Speichern von vertraulichen Daten
- Erstellen virtueller Container zum Speichern vertraulicher Daten

- Verschlüsseln der Daten in logischen Partitionen der Festplatte, einschließlich System- und Bootsektoren, auf Flash Cards, USB-Speichergeräten und ähnlichen Massenspeichergeräten

Der Schutz des Systemlaufwerks gewährleistet die Vertraulichkeit:

- der Daten im Arbeitsspeicher, die beim Übergang in den Ruhemodus auf der Festplatte gespeichert werden
- der Daten in der Speicherauszugsdatei, die bei Abstürzen auf der Festplatte gespeichert werden
- der Daten in temporären und Auslagerungsdateien

### **Arbeitsweise mit geschützten Daten**

Mithilfe des Systems wird Folgendes gewährleistet:

- Beschränkung des Zugriffs auf geschützte Daten durch Einrichtung eines Benutzerkennworts
- Möglichkeit der Speicherung von geschützten Objekten in anderen geschützten Objekten
- Vermeidung von zufälligen oder absichtlichen Beschädigungen geschützter Objekte durch Zugriffsbeschränkungen auf diese Objekte
- Verwendung geschützter Ordner, Container und logischer Festplattenpartitionen auf dem Computer des Benutzers
- Möglichkeit der Übertragung geschützter Objekte (zusammen mit dem physischen Datenträger, auf dem sich die Objekte befinden), auf einen anderen Computer, auf dem das System ebenfalls installiert ist. Dabei können die Objekte weiterhin verwendet werden.
- Sicheres Löschen von Dateien und Ordnern

# 1.1. Komponenten von Kaspersky KryptoStorage

Die Komponenten von Kaspersky KryptoStorage sind in der folgenden Tabelle aufgeführt.

Komponente	Bedeutung der Komponente
Komponenten, die in den Arbeitsplatz (Shell) eingebettet sind	Erstellen geschützter Objekte, Verwenden geschützter Daten, Entschlüsseln von Objekten, sicheres Löschen von Dateien und Ordnern
Steuerung der Anwendung Kaspersky KryptoStorage	Aktivierung und Verwenden von Lizenzen, Einrichten der Subsysteme von Kaspersky KryptoStorage, Erstellen geschützter Objekte, Wiederherstellen geschützter Laufwerke
Kaspersky KryptoStorage-Hilfe	Hilfedatei im Format .CHM

## 1.2. Geschützte Objekte

Unter **geschützten Objekten** sind beliebige Objekte zu verstehen, die zum Speichern der von Kaspersky KryptoStorage verschlüsselten Objekte vorgesehen sind.

**Geschützte Objekte** weisen die folgenden Typen auf.

- **Geschützte Ordner** dienen als spezielle Ordner im NTFS-Dateisystem, die der Benutzer mit Kaspersky KryptoStorage auf seinem Computer einrichtet. Nach dem Erstellen eines solchen Ordners mit Kaspersky KryptoStorage kann er wie gewöhnliche Ordner des NTFS-Dateisystems verwendet werden.

- **Geschützte Container** dienen als spezielle Dateien, die der Benutzer mit Kaspersky KryptoStorage auf seinem Computer erstellt. Nach dem Erstellen eines solchen Containers mit Kaspersky KryptoStorage kann dieser wie virtuelle logische Laufwerke verwendet werden. Darüber hinaus können Containerdateien kopiert, auf CD oder DVD gebrannt, per E-Mail verschickt und auf einen anderen Computer übertragen werden, auf dem das System ebenfalls installiert ist. Dabei kann der Container weiterhin verwendet werden.
- **Geschützte Partitionen (Laufwerke)** werden durch Umwandlung (Verschlüsselung) bestehender logischer Partitionen einer Festplatte mit den darauf gespeicherten Daten durch Kaspersky KryptoStorage erstellt. Auf diese Weise können System - bzw. Bootsektoren sowie Massenspeichergeräte (z.B. Flash Cards und USB-Speichergeräte) verschlüsselt werden. Nach dem Erstellen eines geschützten Laufwerks mit Kaspersky KryptoStorage kann dieses wie gewöhnliche Laufwerke verwendet werden.

#### **Wichtige Informationen!**

Nach dem Erstellen eines geschützten Objekts werden alle darin gespeicherten Daten automatisch durch Verschlüsselung geschützt. Wenn die Daten aus einem geschützten Objekt in einen ungeschützten Bereich kopiert werden, werden sie in diesem ungeschützten Bereich unverschlüsselt gespeichert.

## **1.3. Zugriffsberechtigungen auf geschützte Objekte**

Zur Vorbeugung vor unerwünschten Aktionen ist der Zugriff auf geschützte Objekte erst nach Autorisierung des Benutzers möglich.

Die Autorisierung ist für folgende Aktionen erforderlich:

- Einbindung geschützter Objekte
- Änderung des Kennworts
- Entschlüsselung, Unterbrechung und Fortsetzung des Verschlüsselungsvorgangs, Verschlüsselung, Zurückführung von geschützten Festplattenpartitionen (Laufwerken) in den vorherigen Zustand.

Für die Autorisierung des Benutzers ist es erforderlich, das Kennwort für den Zugriff auf das gegebene Objekt einzugeben.

**Hinweis:**

Wenn der Benutzer ein falsches Kennwort eingegeben hat (weil er es beispielsweise vergessen hat), wird zunächst die Meldung angezeigt, daß der Zugriff verweigert wurde. Danach wird ein Kennworthinweis angezeigt, wenn der Benutzer beim Festlegen des Kennworts einen Hinweis darauf angegeben hat.

## 1.4. Empfehlungen zum Erstellen eines Kennworts und eines Kennworthinweises

Der Zugriff auf geschützte Objekte ist nur nach Autorisierung des Benutzers möglich. Das Kennwort gehört zu den obligatorischen Parametern der Autorisierung. Beim Anlegen des Kennworts sollte Folgendes beachtet werden:

- Das Kennwort sollte mindestens sieben Zeichen enthalten.
- Das Kennwort sollte Ziffern, lateinische Buchstaben, Leerzeichen und Sonderzeichen (z.B. ".", ",", "?", "!", "<", ">" und «"») enthalten.
- Es wird empfohlen, im Kennwort Ziffern und Buchstaben (Groß- und Kleinbuchstaben) zu mischen.

Folgendes sollte nicht im Kennwort enthalten sein:

- Allgemeingebäuchliche Wörter und stehende Redewendungen
- Zeichenfolgen, die sich aus Tasten zusammensetzen, die auf der Tastatur nebeneinander liegen, wie: *qwertz*, *123456789*, *qayxsw* usw.
- Persönliche Daten: Vor- und Nachname, Adresse, Ausweisnummer, Versicherungsnummer usw.
- Außerdem empfiehlt es sich ebenfalls nicht, Kennwörter wiederholt zu verwenden, die auch für den Zugriff auf andere Programme festgelegt wurden (E-Mail-Anwendungen, Datenbanken usw.).

**Wichtige Informationen!**

Im Falle des Kennwortverlusts für den Zugriff auf ein geschütztes Objekt ist die Wiederherstellung des Objekts nicht möglich!

Es besteht die Möglichkeit, einen Kennworthinweis zu verwenden. Bei dem Hinweis handelt es sich um eine Zeichenfolge in dem speziell dafür vorgesehenen Feld, die der Benutzer bei der Festlegung des Kennworts angeben kann. Wenn ein Hinweis angegeben wurde, zeigt das System bei fehlerhafter Eingabe des Kennworts zunächst die Meldung, daß der Zugriff auf das Objekt verweigert wurde und dann den Hinweis an. Der Hinweis sollte Informationen enthalten, durch die sich der Benutzer an sein Kennwort erinnern kann.

**Wichtige Informationen!**

Denken Sie beim Angeben des Hinweises für das Kennwort daran, daß dieser Hinweis allen Benutzern beim Versuch das Objekt aufzurufen, angezeigt wird. Deshalb sollte der Hinweis keinen direkten Verweis auf das Kennwort enthalten.

# KAPITEL 2. KASPERSKY KRYPTOSTORAGE INSTALLIEREN

In diesem Abschnitt sind Informationen zu den Hardware- und Softwarevoraussetzungen sowie eine Beschreibung der Installation und Aktualisierung des Produkts und der Lizenzverwaltung enthalten.

## 2.1. Hardware- und Softwarevoraussetzungen

Für Kaspersky KryptoStorage ist es erforderlich, daß die Computerkonfiguration die folgenden Hardware- und Softwarevoraussetzungen aufweist.

### Hardwarevoraussetzungen:

- Prozessor Intel Pentium mit 1 GHz oder höher
- 256 MB Arbeitsspeicher
- 10 MB freier Festplattenspeicher für die Installation des Programms

### Softwarevoraussetzungen:

- Eines der folgenden Betriebssysteme:
  - Microsoft Windows 2000 (Service Pack 4 + alle Aktualisierungen)
  - Microsoft Windows XP Service Pack 2
  - Microsoft Windows Vista Service Pack 1
  - Microsoft Windows 7

Für Betriebssysteme, die die Plattformen x86 und x64 unterstützen, kann das System in allen Varianten verwendet werden.

## 2.2. Installationsbeschreibung

### Wichtige Informationen!

Für die Installation von Kaspersky KryptoStorage muß der Benutzer über lokale Administratorrechte auf dem Computer verfügen.

Die Installation beginnt mit dem Installationsassistenten. In jedem Fenster sind verschiedene Schaltflächen zum Steuern des Installationsvorgangs verfügbar. Diese werden im Folgenden erläutert:

- **Weiter** – Durch Klicken auf diese Schaltfläche werden die Eingaben übernommen, und der Installationsvorgang wird mit dem nächsten Schritt fortgesetzt.
- **Zurück** – Durch Klicken auf diese Schaltfläche wird zum vorherigen Schritt des Installationsvorgangs zurückgekehrt.
- **Abbrechen** – Durch Klicken auf diese Schaltfläche wird der Installationsvorgang abgebrochen.

Im Folgenden wird der Installationsvorgang des Systems schrittweise erläutert.

### Schritt 1. Vor der Installation

Legen Sie die CD von Kaspersky KryptoStorage in das CD/DVD-Laufwerk ein, oder lassen Sie die Installationsdatei `ksVVVde.exe` selbständig starten.

In der Bezeichnung der Installationsdatei gibt `VVV` die Programmversion des Produkts an.

### Hinweis:

Updates für Kaspersky KryptoStorage können Sie unter folgender Adresse abrufen: <http://www.kaspersky.com/de/downloads>.

Danach erscheint auf dem Bildschirm das Begrüßungsfenster des Installationsassistenten von **Kaspersky KryptoStorage**.

Klicken Sie zum Fortsetzen der Installation auf **Weiter**. Um den Installationsvorgang abzubrechen, klicken Sie auf **Abbrechen**.

### Schritt 2. Lizenzvertrag akzeptieren

Lesen Sie den Text der Lizenzvereinbarung. Für die Fortsetzung des Installationsvorgangs ist es erforderlich, die Bedingungen des Lizenzvertrags zu akzeptieren und auf **Weiter** zu klicken.

### Schritte 3. Installationsordner auswählen

Im Fenster **Zielordner** wird im entsprechenden Feld der Pfad zu dem Ordner angezeigt, in dem Kaspersky KryptoStorage installiert wird.

Sie können einen anderen Ordner auswählen, indem Sie auf die Schaltfläche **Ändern...** klicken und im Auswahlfenster einen Ordner auswählen oder den Pfad des Ordners in das entsprechende Eingabefeld eingeben.

Klicken Sie zum Fortsetzen der Installation auf **Weiter**.

### Schritt 4. Installation abschließen

Klicken Sie in dem daraufhin angezeigten Fenster **Programmvorbereitungen zur Installation abgeschlossen** auf die Schaltfläche **Installieren**, um Kaspersky KryptoStorage zu installieren.

Befolgen Sie die weiteren Anweisungen im Installationsassistenten, um die Installation von Kaspersky KryptoStorage abzuschließen.

Nach Abschluß der Installation müssen Sie das Produkt aktivieren. Dazu können Sie eine der folgenden Varianten wählen:

- Aktivieren der Testversion für 30 Tage
- Aktivieren der Vollversion

Für die Aktivierung der Vollversion ist es erforderlich, einen Lizenzschlüssel über den Aktivierungscode abzurufen und zu installieren. Informationen zum Abrufen und Installieren des Lizenzschlüssels über den Aktivierungscode finden Sie in Abschnitt 2.4 auf Seite 16. Klicken Sie nach Auswahl des Aktivierungstyps auf **Weiter**.

Damit die Installation korrekt abgeschlossen wird, muß der Computer neu gestartet werden. Auf dem Bildschirm wird eine entsprechende Meldung angezeigt.

#### **Wichtige Informationen!**

Unterbrechen Sie während des Neustarts nicht die Stromversorgung (solange Microsoft Windows ausgeführt wird). Dies kann beim Hochfahren des Betriebssystems zu Fehlern führen.

Falls die Stromversorgung unterbrochen wurde, drücken Sie beim Hochfahren des Betriebssystems die Taste **F8** und wählen in dem angezeigten Menü den Befehl **Letzte als funktionierend bekannte Konfiguration**. Installieren Sie Kaspersky KryptoStorage anschließend erneut.

## 2.3. Lizenzverwaltung

Damit Kaspersky KryptoStorage mit voller Funktionalität ausgeführt wird, ist es erforderlich, eine kommerzielle Lizenz zu erwerben und zu registrieren.

### Hinweis:

Durch Aktivierung der Testversion können Sie 30 Tage lang alle Funktionen von Kaspersky KryptoStorage mit einem auf 1 Zeichen beschränktes Kennwort nutzen.

Nach Ablauf der Gültigkeitsdauer der Testlizenz wird der Funktionsumfang des Produkts teilweise eingeschränkt. Der Benutzer kann weiterhin die bereits erstellten (geschützten) Objekte verwenden. Weiterhin ist er in der Lage, beim Datenzugriff seine Daten zu entschlüsseln. Er kann jedoch keine neuen geschützten Objekte erstellen und auch nicht den technischen Support in Anspruch nehmen.

### So starten Sie die Lizenzverwaltung von Kaspersky KryptoStorage:

1. Klicken Sie auf **Start**, und wählen Sie **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage** aus.
2. Klicken Sie in dem daraufhin angezeigten Fenster auf die Schaltfläche **Lizenzen**.

Auf dem Bildschirm wird das Dialogfenster **Lizenzen** angezeigt (siehe Abb. 1).

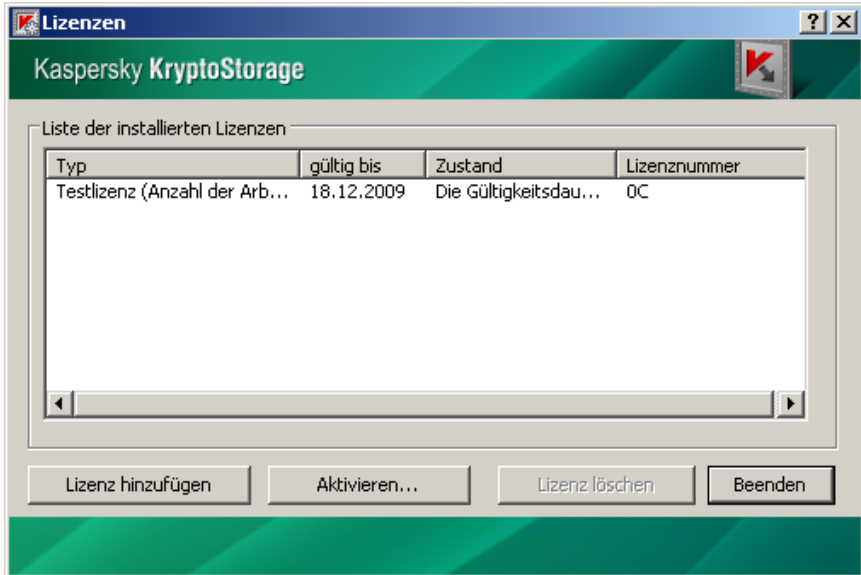


Abb. 1: Lizenzen

Das Fenster enthält eine Liste der installierten Lizenzen zusammen mit dem jeweiligen Typ, der zugehörigen Seriennummer, dem aktuellen Status und der Gültigkeitsdauer.

Um weitere, zuvor erworbene Lizenzen zu dieser Liste hinzuzufügen, klicken Sie auf **Lizenz hinzufügen**. Geben Sie in dem daraufhin angezeigten Dialogfenster den Pfad zu der Lizenzdatei an, und klicken Sie auf **Öffnen**.

**Hinweis:**

Das Hinzufügen von Lizenzen ist vom Benutzer auszuführen, dem auch die anderen Lizenzen in der Liste gehören. Andernfalls ist das Hinzufügen von Lizenzen nicht möglich.

Um eine nicht mehr benötigte Lizenz aus der Liste zu löschen, wählen Sie diese aus und klicken auf **Lizenz löschen**.

**Hinweis:**

Testlizenzen können nicht aus der Liste der installierten Lizenzen gelöscht werden.

**Wichtige Informationen!**

Löschen Sie aus der Liste keine aktive kommerzielle Lizenz, da dadurch der Funktionsumfang des Produkts wie bei Ablauf der Gültigkeitsdauer der Testlizenz eingeschränkt wird.

Um einen Lizenzschlüssel über den Aktivierungscode abzurufen und zu installieren, klicken Sie auf **Aktivieren**. Informationen zum Aktivieren von Lizenzen über den Aktivierungscode finden Sie unter 2.4 auf Seite 16.

Nachdem Sie die Bearbeitung der Liste mit den installierten Lizenzen abgeschlossen haben, schließen Sie das Fenster durch Klicken auf **Beenden**.

## 2.4. Lizenzschlüssel mit Aktivierungscode abrufen und installieren

Die Verwendung von Aktivierungscodes zum Abrufen und Installieren von Lizenzschlüsseln ist sowohl während als auch nach der Installation des Produkts (im Zuge der Lizenzverwaltung) möglich (siehe Abschnitt 2.3 auf Seite 14).

**Wichtige Informationen!**

Damit Sie einen Lizenzschlüssel durch Eingabe des Aktivierungscodes abrufen können, muß Ihr Computer mit dem Internet verbunden sein, um auf den Lizenzservice zugreifen zu können.

Geben Sie zum Abrufen des Lizenzschlüssels in das angezeigte Fenster den Aktivierungscode des Produkts ein, der aus fünf Teilen besteht. Dabei umfaßt jeder Teil des Codes wiederum fünf Zeichen (siehe Abb. 2), die aus Ziffern (außer 0) und lateinischen Großbuchstaben bestehen.

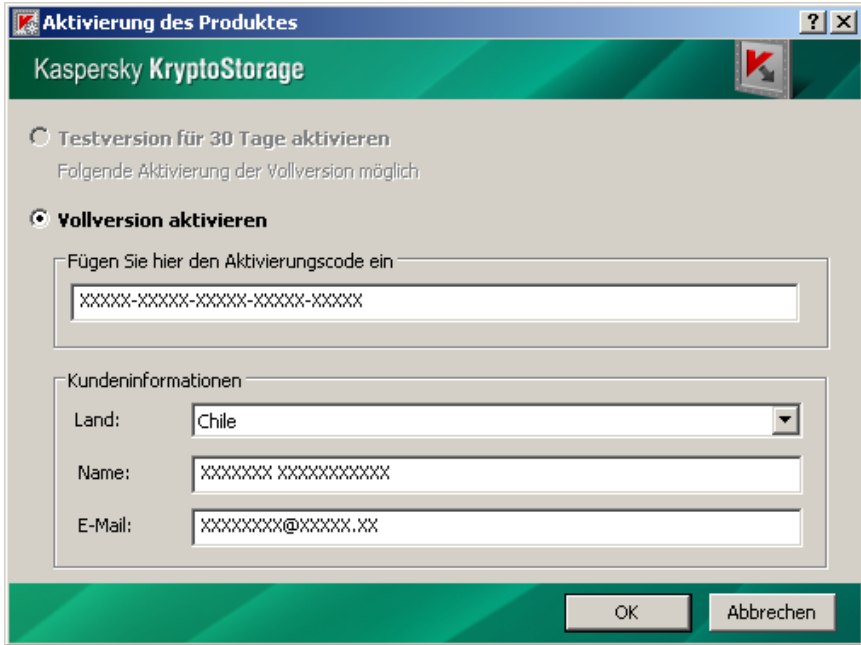


Abb. 2: Produktaktivierung

Geben Sie anschließend im Informationsbereich über den Käufer Ihr Heimatland an. Optional können Sie auch Ihren Namen und Ihre E-Mail-Adresse angeben. Klicken Sie abschließend auf **OK**.

Die weiteren Operationen zum Abrufen und Installieren von Lizenzschlüsseln werden automatisch ausgeführt.

### **Wichtige Informationen!**

Für jeden Aktivierungscode wird nur ein Lizenzschlüssel ausgegeben. Geben Sie deshalb in keinem Fall den Aktivierungscode Ihres Produkts preis.

Kopieren Sie die erhaltene Lizenzdatei auf ein anderes physisches Laufwerk oder auf einen Wechseldatenträger. Sie benötigen diese Kopie möglicherweise nach einer Störung zur Wiederherstellung des Systems.

## 2.5. Produktversion aktualisieren

Updates für Kaspersky KryptoStorage können Sie unter folgender Adresse abrufen: <http://www.kaspersky.com/de/downloads>.

Starten Sie zur Aktualisierung Ihres Produkts das Installationsprogramm des Updates.

**Hinweis:**

Eine neuere Produktversion kann nicht über eine ältere Version installiert werden. Für diesen Vorgang muß zunächst die derzeit installierte Version des Produkts deinstalliert werden (siehe Kapitel 6 auf Seite 51).

# KAPITEL 3. BENUTZER-OBERFLÄCHE DES SYSTEMS

In diesem Abschnitt wird die Benutzeroberfläche des Systems detailliert erläutert.

## 3.1. Kontextmenü im Explorer

Unter Microsoft Windows erfolgt der Zugriff auf die Funktionen des Systems über ein Kontextmenü im Explorer.

**So öffnen Sie das Menü Kaspersky KryptoStorage:**

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt (Ordner, Container, logische Laufwerkspartition).
2. Wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage** (siehe Abb. 3).

Durch Klicken auf diese Option wird ein Untermenü geöffnet, dessen Inhalt vom ausgewählten Objekttyp und davon abhängt, ob das jeweilige Objekt geschützt ist.

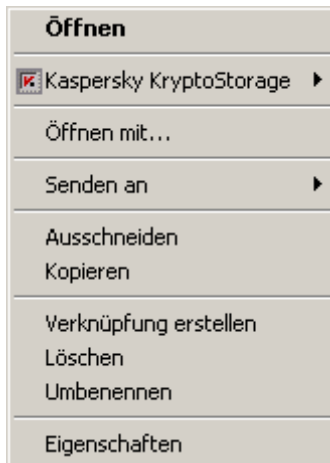


Abb. 3: Menü Kaspersky KryptoStorage

**So erstellen Sie einen geschützten Ordner oder einen geschützten Container:**

Klicken Sie mit der rechten Maustaste auf eine beliebige freie Stelle im geöffneten Ordner bzw. im Arbeitsplatz, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Neu ► Kaspersky KryptoStorage-Ordner** oder **Neu ► Kaspersky KryptoStorage-Container** aus.

## **3.2. Fenster der Steuerung von Kaspersky KryptoStorage**

**So starten Sie die Steuerung von Kaspersky KryptoStorage:**

Klicken Sie auf **Start**, und wählen Sie **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage** aus.

Daraufhin wird das Fenster der Anwendungssteuerung angezeigt (siehe Abb. 4).

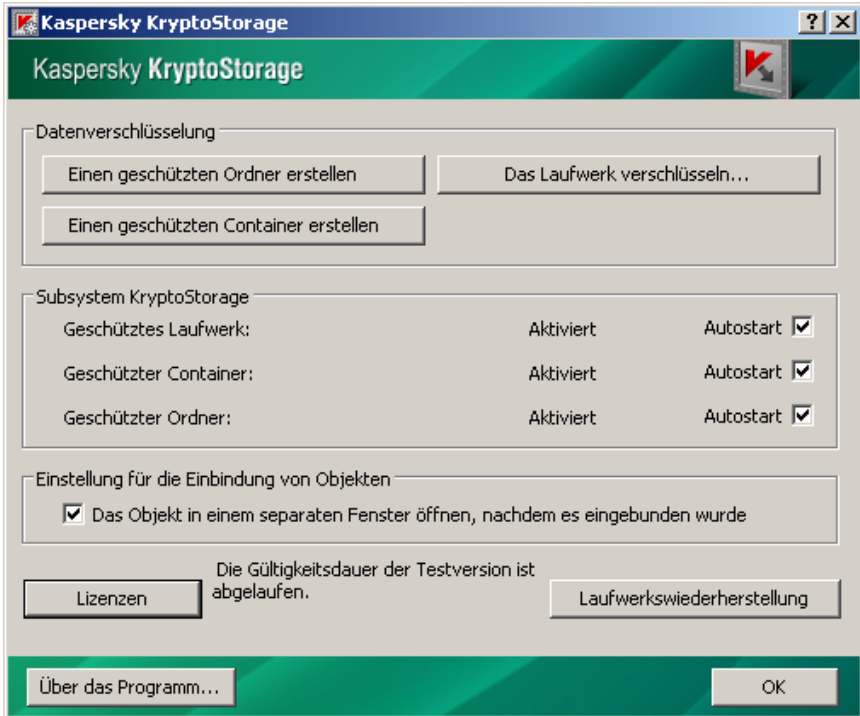


Abb. 4: Fenster der Anwendungssteuerung

Über dieses Fenster können Sie die folgenden Operationen ausführen:

- Erstellen geschützter Ordner (siehe Abschnitt 4.1.1 auf Seite 23)
- Erstellen geschützter Container (siehe Abschnitt 4.2.1 auf Seite 28)
- Verschlüsseln von Laufwerken (siehe Abschnitt 4.3.2 auf Seite 38)
- Konfigurieren von Subsystemen (siehe Abschnitt 5 auf Seite 48)
- Möglichkeit zum Öffnen eines Objekts in einem separaten Explorer-Fenster, nachdem es eingebunden wurde
- Verwenden von Lizenzen, Aktivierungen (siehe Abschnitt 2.3 auf Seite 14)
- Wiederherstellen geschützter Partitionen (siehe Abschnitt 4.3.10 auf Seite 45)

# KAPITEL 4. DATENSCHUTZ DURCH DIE VERWENDUNG GESCHÜTZTER OBJEKTE

In diesem Kapitel wird die Verwendung der folgenden geschützten Objekte erläutert:

- Geschützte Ordner (siehe Abschnitt 4.1 auf Seite 22)
- Geschützte Container (siehe Abschnitt 4.2 auf Seite 28)
- Geschützte logische Festplattenpartitionen und Wechseldatenträger (siehe Abschnitt 4.3 auf Seite 35).

## 4.1. Geschützte Ordner

Voraussetzungen zum Erstellen von geschützten Ordnern:

- Die Verwendung von geschützten Ordnern ist möglich, wenn auf dem Computer, auf dem Kaspersky KryptoStorage installiert ist, das Subsystem *Geschützte Ordner* ausgeführt wird (für Informationen zum Subsystem siehe Kapitel 5 auf Seite 48). Standardmäßig wird das Subsystem ausgeführt.
- Das Laufwerk (Festplatte oder Wechseldatenträger), auf dem der geschützte Ordner erstellt werden soll, darf nicht schreibgeschützt sein. Der Benutzer, der den geschützten Ordner erstellen möchte, muß über die entsprechenden Rechte verfügen.
- Geschützte Ordner können nur in einem NTFS-Dateisystem erstellt werden.
- Sie können nicht in einem geschützten Kaspersky KryptoStorage-Ordner erstellt werden.
- Sie können nicht in einem mit EFS verschlüsselten Ordner (verschlüsselndes Dateisystem, das zum Betriebssystem Microsoft Windows gehört) erstellt werden.
- Der Name des Ordners darf maximal 255 Zeichen aufweisen.

## 4.1.1. Ordner erstellen

### Wichtige Informationen!

Machen Sie sich zunächst mit den Besonderheiten beim Erstellen von geschützten Ordnern vertraut, die in Abschnitt 4.1 auf Seite 22 erläutert werden.

Sie können geschützte Ordner auf der Festplatte oder auf einem Wechseldatenträger erstellen. Darüber hinaus können Sie geschützte Ordner innerhalb eines anderen geschützten Objekts (auf einem logischen Laufwerk oder in einem geschützten Container) erstellen.

### Hinweis:

Wenn Sie einen Ordner innerhalb eines anderen geschützten Objekts erstellen, muß dieses Objekt vor dem Erstellen des Ordners eingebunden werden.

### So erstellen Sie einen geschützten Ordner:

1. Führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie mit der rechten Maustaste auf eine beliebige freie Stelle im geöffneten Ordner bzw. im Arbeitsplatz, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Neu ► Kaspersky KryptoStorage-Ordner**.
  - Starten Sie die Anwendung Kaspersky KryptoStorage, indem Sie im Menü **Start** auf **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage** klicken und in dem daraufhin angezeigten Fenster auf die Schaltfläche **Einen Geschützten Ordner erstellen** klicken.

Daraufhin wird auf dem Bildschirm das Dialogfenster **Geschützten Ordner erstellen** angezeigt (siehe Abb. 5).

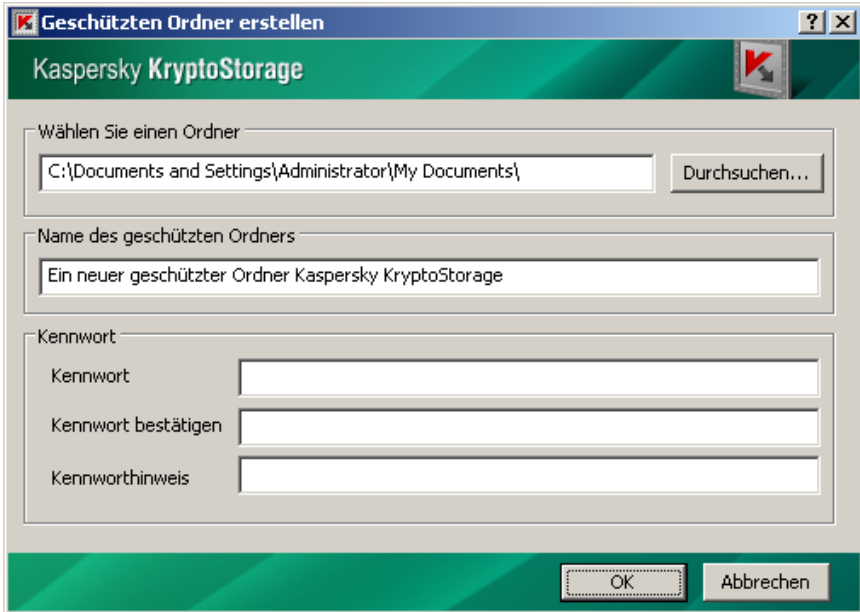


Abb. 5: Geschützten Ordner erstellen

2. Geben Sie die Parameter für den zu erstellenden geschützten Ordner ein:
  - **Wählen Sie einen Ordner:** Geben Sie den Ordner an, in dem der geschützte Ordner erstellt werden soll. Wenn der geschützte Ordner über das Kontextmenü im Explorer erstellt wird, wird er an dem Ort erstellt, an welchem das Menü aufgerufen wurde. Wenn der geschützte Ordner über das Fenster der Anwendung erstellt wird, wird standardmäßig der Ordner **Eigene Dateien** des Benutzerprofils angegeben. In beiden Fällen besteht die Möglichkeit, einen anderen Ordner zu wählen.
  - **Name des geschützten Ordners:** Geben Sie einen Namen für den geschützten Ordner ein.

**Hinweis:**

Sie können die Namen geschützter Ordner mithilfe der herkömmlichen Betriebssystemfunktionen jederzeit ändern.

- **Kennwort, Kennwort bestätigen, Kennworthinweis:** Geben Sie das Kennwort für den Zugriff auf den geschützten Ordner und (optional) einen Kennworthinweis an. Diese Parameter werden für den Zugriff auf den Ordner verwendet.

**Hinweis:**

Empfehlungen zur Einrichtung von Kennwort und Kennworthinweis finden Sie in Abschnitt 1.4 auf Seite 9.

3. Klicken Sie auf **OK**, nachdem Sie alle erforderlichen Parameter angegeben haben.

Daraufhin wird der geschützte Ordner erstellt. Der Ordner ist nach seiner Erstellung eingebunden und kann verwendet werden.

## 4.1.2. Regeln zur Verwendung geschützter Ordner

Bei der Verwendung geschützter Ordner sind folgende Regeln zu beachten:

- Alle Dateien und Ordner, die sich in einem geschützten Ordner befinden, sind verschlüsselt und dadurch geschützt.
- Die Ausführung beliebiger Aktionen (lesen, speichern, umbenennen, archivieren, löschen usw.) im geschützten Ordner ist nur möglich, nachdem der entsprechende Ordner eingebunden wurde.
- Auf den eingebundenen Ordner können alle Benutzer und Programme zugreifen, die mit dem Benutzernamen, der den Ordner eingebunden hat, lokal auf dem Computer arbeiten können. Der Zugriff auf geschützte Ordner über ein Netzwerk ist durch das System verboten.

**Hinweis:**

Es empfiehlt sich, geschützte Ordner sofort wieder zu trennen, nachdem Sie deren Verwendung abgeschlossen haben.

- Kopierte oder verschobene Dateien und Ordner weisen nur den Schutz der Objekte auf, in denen Sie sich befinden.

**Hinweis:**

Kopierte oder verschobene Dateien und Ordner, die sich in ungeschützten Systemobjekten befinden, sind ebenfalls nicht geschützt.

- Das System erlaubt es nicht, die folgenden Aktionen direkt mit geschützten Ordnern und den darin enthaltenen Objekten auszuführen: Verschieben in den Papierkorb, Verschieben innerhalb eines Laufwerks mit Dateien und Ordnern, die Dateien enthalten.

**Hinweis:**

Bei dem Versuch, einen Ordner mit Dateien innerhalb eines Laufwerks zu verschieben, bleibt der ursprüngliche Ordner unverändert erhalten. Am neuen Speicherort wird ein leerer Ordner mit dem Namen des ursprünglichen Ordners erstellt, der den Schutz des Objekts aufweist, in dem er sich befindet.

Einige Datei-Manager (z.B. Total Commander) verwenden beim Verschieben von Dateien und Ordnern innerhalb eines Laufwerks die Kopierfunktion, wobei die ursprünglichen Objekte anschließend gelöscht werden. In diesem Fall ist das Verschieben möglich, wobei die verschobenen Dateien und Ordner nur den Schutz der Objekte aufweisen, in denen sie sich befinden.

- Innerhalb eines Laufwerks können ungeschützte Ordner, die geschützte Unterordner enthalten, mit ihrem gesamten Inhalt verschoben werden. In diesem Fall ist es für das Verschieben von Objekten nicht erforderlich, daß diese eingebunden werden. Außerdem werden alle Eigenschaften der geschützten Objekte gespeichert.
- Ein ungeschützter Ordner, der geschützte Unterordner enthält, kann möglicherweise in den Papierkorb verschoben werden, wenn alle geschützten Objekte im Ordner eingebunden sind.

**Hinweis:**

In den Papierkorb verschobene geschützte Ordner können gelöscht oder wiederhergestellt werden. Bei der Wiederherstellung werden alle geschützten Objekte des Ordners eingebunden. Nachdem Sie einen Neustart des Computers durchgeführt oder sich abgemeldet haben, können Sie den in den Papierkorb verschobenen Ordner nur noch wiederherstellen und nicht mehr löschen. Bei seiner Wiederherstellung werden alle geschützten Objekte des Ordners getrennt. Unter Microsoft Windows Vista und Microsoft Windows 7 können Sie nach einem Neustart des Computers oder nach der Abmeldung Ordner löschen und aus dem Papierkorb wiederherstellen.

In Total Commander ist das Verschieben eines solchen Ordners in den Papierkorb nicht möglich.

## 4.1.3. Geschützte Ordner einbinden

Geschützte Ordner müssen eingebunden sein, damit sie verwendet (z.B. gelesen, gespeichert, umbenannt, kopiert und gelöscht) werden können.

**So binden Sie einen Ordner ein:**

1. Wählen Sie den geschützten Ordner aus, den Sie einbinden möchten.
2. Klicken Sie mit der rechten Maustaste auf den ausgewählten Ordner, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Den Ordner einbinden** aus.
3. Geben Sie in das daraufhin angezeigte Dialogfenster das Kennwort für den Zugriff auf den geschützten Ordner ein.
4. Klicken Sie auf **OK**.

## 4.1.4. Geschützte Ordner trennen

Durch Trennen wird ein geschützter Ordner wieder in den Zustand versetzt, in dem er nicht bearbeitet werden kann, bis er wieder eingebunden wird.

### **Wichtige Informationen!**

Geschützte Ordner dürfen erst getrennt werden, nachdem alle daran durchgeführten Änderungen gespeichert wurden. Dies steht im Zusammenhang damit, daß Anwendungen den Datenzugriff bis zum Abschluß aller Operationen an diesen Daten speichern können.

**So trennen Sie einen geschützten Ordner:**

1. Wählen Sie den geschützten Ordner aus, dessen Bearbeitung abgeschlossen ist.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Den Ordner trennen** aus.

Wenn gleichzeitig mehrere geschützte Objekte verwendet werden, nimmt das Trennen von allen Objekten eine gewisse Zeit in Anspruch. Es können jedoch auch Situationen auftreten, in denen es erforderlich ist, alle geschützten Objekte gleichzeitig zu trennen. Dies bewirken Sie durch einen Neustart des Computers (nachdem Sie alle durchgeführten Änderungen gespeichert haben). Nach dem Neustart des Computers sind alle geschützten Objekte abgehängt. Sie können alle geschützten Ordner auch abhängen, indem Sie sich vom System abmelden.

## 4.2. Geschützte Container

Das Laufwerk (Festplatte oder Wechseldatenträger), auf dem ein geschützter Container erstellt werden soll, darf nicht schreibgeschützt sein. Der Benutzer, der den geschützten Container erstellen möchte, muß über die entsprechenden Rechte verfügen.

Das Erstellen von geschützten Containern auf CD/DVD wird nicht unterstützt. Diese Datenträger können jedoch zum Speichern von vorbereiteten geschützten Containern verwendet werden.

Die Verwendung von geschützten Containern ist nur dann möglich, wenn auf dem Computer, auf dem Kaspersky KryptoStorage installiert ist, das Subsystem *Geschützte Container* ausgeführt wird.

### 4.2.1. Container erstellen

#### Wichtige Informationen!

Machen Sie sich zunächst mit den Besonderheiten beim Erstellen von geschützten Containern vertraut, die in Abschnitt 4.2 auf Seite 28 erläutert werden.

Sie können Container auf der Festplatte oder auf einem Wechseldatenträger erstellen. Darüber hinaus können Sie geschützte Container innerhalb eines anderen geschützten Objekts (auf einem logischen Laufwerk, auf einem Wechseldatenträger, in einem Ordner oder in einem geschützten Container) erstellen.

#### Hinweis:

Wenn Sie einen Container innerhalb eines anderen geschützten Objekts erstellen, muß dieses Objekt vor dem Erstellen des Containers eingebunden werden.

#### So erstellen Sie einen Container:

1. Führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie mit der rechten Maustaste auf eine beliebige freie Stelle im geöffneten Ordner bzw. im Arbeitsplatz, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Neu ► Kaspersky KryptoStorage-Ordner** aus.

- Starten Sie die Anwendung Kaspersky KryptoStorage, indem Sie **Start** und dann **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage** auswählen, und klicken Sie in dem daraufhin angezeigten Fenster auf **Einen geschützten Container erstellen**.

Daraufhin wird auf dem Bildschirm das Dialogfenster **Erstellen eines geschützten Containers** angezeigt (siehe Abb. 6).

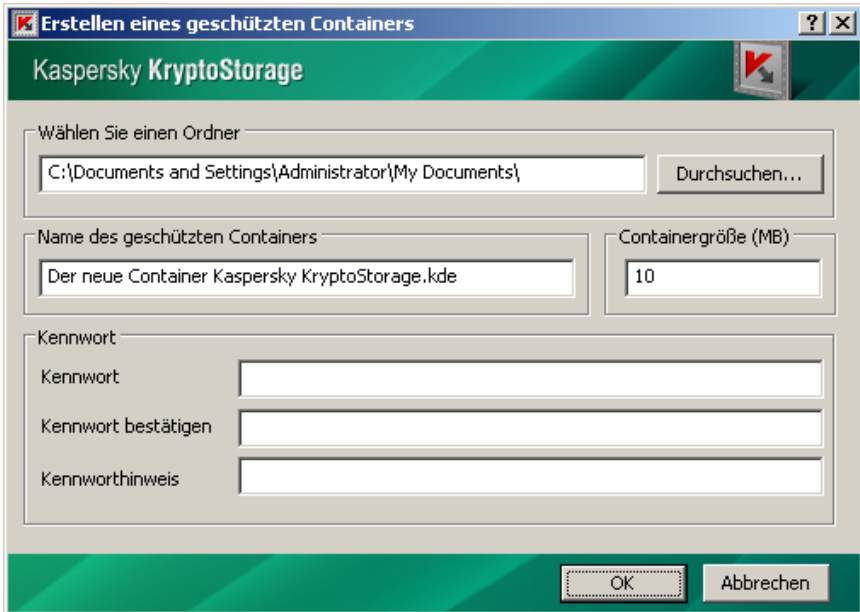



Abb. 6: Geschützten Container erstellen

2. Geben Sie die Parameter für den zu erstellenden geschützten Container ein:
  - **Wählen Sie einen Ordner:** Geben Sie den Ordner an, in dem der geschützte Container erstellt werden soll. Wenn der Container über das Kontextmenü im Explorer erstellt wird, wird in diesem Feld der Ordner angegeben, über den das Menü aufgerufen wurde. Wenn der Container über das Fenster der Anwendungssteuerung erstellt wird, wird in diesem Feld der Ordner **Eigene Dateien** des Benutzerprofils angegeben. In beiden Fällen besteht die Möglichkeit, einen anderen Ordner zu wählen.

- **Name des geschützten Containers:** Geben Sie den Namen und die Erweiterung der Datei des geschützten Containers an.

Standardmäßig weist die Datei des Containers die Erweiterung `.kde` auf (bei der Installation von Kaspersky KryptoStorage werden Dateien mit dieser Erweiterung im Betriebssystem als Kaspersky KryptoStorage-Container registriert). Im Betriebssystem werden derartige Dateien mit dem Symbol  angezeigt.

Wenn anstelle von `.kde` eine andere Erweiterung angegeben wird, die im Betriebssystem nicht registriert ist, wird die Containerdatei als Datei mit unbekanntem Format angezeigt.

**Hinweis:**

Das Einbinden von Containerdateien mit der Erweiterung `.kde` unterscheidet sich vom Einbinden von Containerdateien mit einer anderen Erweiterung (siehe Abschnitt 4.2.4 auf Seite 31).

Sie können die Namen und die Erweiterung von Containerdateien mithilfe der Funktionen des Betriebssystems jederzeit ändern.

- **Containergröße:** Größe des Containers in MB.
- **Kennwort, Kennwort bestätigen, Kennwordhinweis:** Geben Sie das Kennwort für den Zugriff auf den geschützten Container und (optional) einen Kennwordhinweis an. Diese Parameter werden für den Zugriff auf den Container verwendet.

**Hinweis:**

Empfehlungen zur Einrichtung des Kennworts und eines Kennwordhinweises finden Sie in Abschnitt 1.4 auf Seite 9.

3. Klicken Sie auf **OK**, nachdem Sie alle erforderlichen Parameter angegeben haben.

Nachdem Sie den geschützten Container erstellt haben, können Sie ihn einbinden (siehe Abschnitt 4.2.44 auf Seite 31) und formatieren (siehe Abschnitt 4.2.5 auf Seite 33).

## 4.2.2. Verwendung vorbereiten

Für die Vorbereitung von Containern für deren Verwendung sind folgende Schritte auszuführen:

1. Container einbinden (siehe Abschnitt 4.2.4 auf Seite 31)
2. Logisches Laufwerk formatieren, auf dem der geschützte Container eingebunden wird (siehe Abschnitt 4.2.5 auf Seite 33).

## 4.2.3. Regeln für die Verwendung von Containern

Die Ausführung beliebiger Aktionen an einem geschützten Container ist erst möglich, nachdem er eingebunden wurde.

### Wichtige Informationen!

Das Einbinden und Verwenden von geschützten Containern ist nur dann möglich, wenn auf dem Computer, auf dem Kaspersky KryptoStorage installiert ist, das Subsystem *Geschützte Container* ausgeführt wird.

Eingebundene Container sind nicht geschützt, sodass alle Benutzer eines Computers darauf zugreifen können. Deshalb ist es unerlässlich, geschützte Objekte sofort wieder zu trennen, nachdem Sie diese verwendet haben.

Bei der Verwendung eines geschützten Containers ist sicherzustellen, daß alle Dateien und Ordner in dem geschützten Container verschlüsselt und geschützt sind. Um diese Objekte aus dem Container verschieben zu können, müssen Sie diese entschlüsseln.

## 4.2.4. Container einbinden

Geschützte Container können erst verwendet werden, nachdem sie eingebunden wurden.

**So binden Sie einen geschützten Container ein:**

1. Wählen Sie den geschützten Container aus.
2. Klicken Sie mit der rechten Maustaste auf den ausgewählten Container, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Container einbinden** aus.

**Hinweis:**

Wenn die Containerdatei die Erweiterung `.kde` aufweist (durch das Symbol  gekennzeichnet), können Sie den Container einbinden, indem Sie doppelt mit der linken Maustaste darauf klicken.

3. Geben Sie in dem daraufhin angezeigten Dialogfenster das Kennwort für den Zugriff auf den geschützten Container ein.
4. Klicken Sie dann auf **OK**.

Daraufhin wird auf dem Bildschirm das Dialogfenster **Containerparameter** angezeigt (siehe Abb. 7).

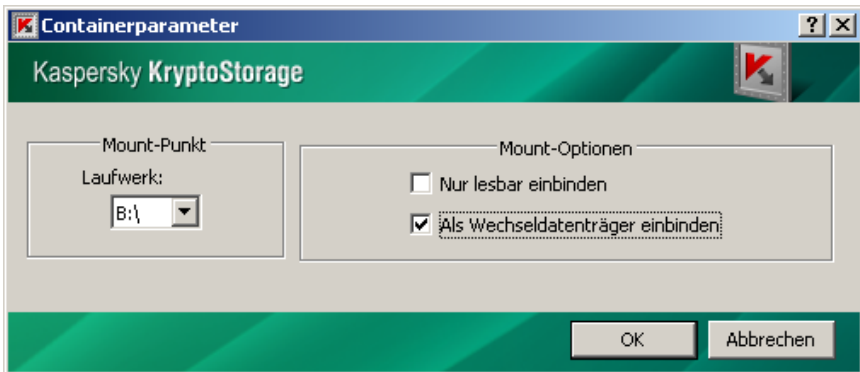


Abb. 7: Parameter für geschützte Container einstellen

5. Geben Sie in dem daraufhin angezeigten Dialogfenster die Parameter für die Einbindung an:
  - **Mount-Punkt:** Wählen Sie den Punkt zum Einbinden des geschützten Containers aus. Als ein derartiger Mount-Punkt kann ein logisches Laufwerk dienen (es kann ein beliebiger, nicht verwendeter Buchstabe eines logischen Laufwerks angegeben werden).
  - **Mount-Optionen:** Parameter zum Einbinden eines geschützten Containers (die Auswahl ist nicht möglich, wenn Container nicht formatiert ist):
    - **Nur lesbar einbinden:** Wenn dieses Kontrollkästchen aktiviert ist, ist der Inhalt des geschützten Containers schreibgeschützt. Damit kann im Container auch nichts gespeichert und nichts daraus gelöscht werden.

**Hinweis:**

Das Kontrollkästchen wird automatisch aktiviert und diese Einstellung kann auch nicht geändert werden, wenn die Containerdatei das Attribut *Schreibgeschützt* aufweist.

Unter Microsoft Windows 2000 ist die Verwendung von *Nur lesbar* mit geschützten Containern, die im NTFS-Dateisystem formatiert wurden, nicht möglich.

- **Als Wechseldatenträger einbinden:** Standardmäßig handelt es sich bei dem Mountpunkt für einen geschützten Container um einen Wechseldatenträger (das in der Liste der Wechseldatenträger im Fenster **Arbeitsplatz** angezeigt wird). Wenn dieses Kontrollkästchen jedoch deaktiviert ist, wird der geschützte Container als Festplatte angesehen (und im **Arbeitsplatz** in der Auflistung der Festplatten angezeigt).

6. Klicken Sie auf **OK**, nachdem Sie alle erforderlichen Parameter angegeben haben.

Beim Einbinden eines erstellten und noch nicht formatierten Containers können Sie die Formatierung durchführen (siehe Abschnitt 4.2.5 auf Seite 33).

## 4.2.5. Container formatieren

**Wichtige Informationen!**

Während der Formatierung des Laufwerks, in dem ein geschützter Container eingebunden ist, werden alle in dem geschützten Container gespeicherten Daten gelöscht.

Benutzer eines geschützten Containers können den eingebundenen Container so formatieren, wie auch Laufwerke formatiert werden. Für die Formatierung werden die Standardfunktionen von Microsoft Windows verwendet. Zum Einrichten der Parameter für die Formatierung ist Folgendes anzugeben:

- Die Verwendung von **Nur lesbar einbinden** ist nicht möglich mit geschützten Containern.
- Damit ein Container unter Microsoft Windows 2000 mit FAT und FAT32 formatiert werden kann, müssen Sie ihn als Wechseldatenträger einbinden und beim Einbinden das Kontrollkästchen **Als Wechseldatenträger einbinden** aktivieren.
- Bei der vollständigen Formatierung weist die Datei des geschützten Containers die Größe auf, die bei der Erstellung des Containers angegeben wurde.

- Bei der schnellen Formatierung und Auswahl des Dateisystems FAT, FAT32 oder exFAT weist die Datei des geschützten Containers immer die Mindestgröße auf, die sich mit jedem im Container gespeicherten Objekt erhöht. Auf diese Weise wird der freie Speicherplatz optimal genutzt.
- Wenn bei der schnellen Formatierung des Dateisystems das Dateisystem NTFS gewählt wird, weist die Datei des geschützten Containers die Größe auf, die während der Erstellung des Containers angegeben wurde.

**Hinweis:**

Bei allen Formatierungsvorgängen entspricht die Größe des geschützten Containers als virtuelles Laufwerk immer der Größe, die während der Erstellung des Containers ausgewählt wurde. Es ändert sich lediglich die Größe der Containerdatei selbst.

**Wichtige Informationen!**

Bei der Verwendung des Containers erhöht sich die Größe der Datei durch das Speichern von Objekten im Container, so daß die Situation auftreten kann, daß auf dem logischen Laufwerk, auf dem der geschützte Container gespeichert ist, kein Speicherplatz mehr verfügbar ist. In diesem Fall besteht die Möglichkeit, die Daten an einem anderen Speicherort zu speichern. Wenn das logische Laufwerk, das zum Speichern der Daten vorgeschlagen wird, nicht geschützt ist, sind auch die darin gespeicherten Daten nicht geschützt. Beim Speichern in einem geschützten Bereich (auf einem anderen logischen Laufwerk oder einem Wechsellaufwerk) werden die Daten wie die anderen Objekte geschützt, die sich in dem geschützten Bereich befinden.

## 4.2.6. Container trennen

Beim Trennen eines geschützten Containers dürfen keine darin enthaltenen Objekte (Dateien, Ordner, untergeordnete geschützte Container) mehr verwendet werden.

**So trennen Sie einen geschützten Container:**

1. Wählen Sie das logische Laufwerk aus, auf dem der geschützte Container eingebunden bzw. auf dem die Datei des geschützten Containers gespeichert ist.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Container trennen** aus.

Wenn gleichzeitig mehrere geschützte Objekte verwendet werden, nimmt das Trennen von allen Objekten eine gewisse Zeit in Anspruch. Es können jedoch auch besondere Situationen auftreten, für die es erforderlich ist, alle geschützten Objekte gleichzeitig zu trennen. Hierfür können Sie einen Neustart des Computers ausführen (nachdem Sie alle durchgeführten Änderungen gespeichert haben). Nach dem Neustart des Computers sind alle geschützten Container getrennt.

## 4.2.7. Löscheschutz

Da es sich bei geschützten Containern um gewöhnliche Dateien handelt, können sie von jedem beliebigen Benutzer gelöscht werden. Um das unbeabsichtigte Löschen von geschützten Containern zu verhindern, können Sie die Containerdatei in einen geschützten Ordner oder auf ein geschütztes logisches Laufwerk verschieben.

### **Wichtige Informationen!**

Diese Art des Schutzes ist nur auf Computern wirksam, auf denen Kaspersky KryptoStorage installiert ist.

## 4.3. Logische Festplattenpartitionen und Wechseldatenträger verschlüsseln

Logische Festplattenpartitionen (einschließlich System- und Bootsektoren) und andere Massenspeichergeräte können verschlüsselt werden.

Geschützte logische Festplattenpartitionen und geschützte Wechseldatenträger weisen die folgenden Besonderheiten auf:

- Wenn eine logische Partition verschlüsselt wird, bei der es sich um einen System- bzw. Bootsektor handelt, erfolgt die Autorisierung für den Zugriff auf die geschützte Partition vor dem Start des Betriebssystems (für weitere Informationen siehe Abschnitt 4.3.7 auf Seite 43).

- Darüber hinaus wird durch die Installation von Kaspersky KryptoStorage auf der Systempartition der Festplatte sichergestellt, daß die Speicherauszugsdatei und der Inhalt des Arbeitsspeichers verschlüsselt werden, die beim Übergang in den Ruhemodus auf dem Systemlaufwerk gespeichert werden. Durch die Verschlüsselung der Systempartition kann dem Diebstahl der auf der Festplatte gespeicherten vertraulichen Daten beim Speichern von Dienstinformationen vorgebeugt werden.
- Die Verwendung von geschützten Laufwerken und Wechseldatenträgern ist möglich, wenn auf dem Computer, auf dem Kaspersky KryptoStorage installiert ist, das Subsystem *Geschützte Laufwerke* ausgeführt wird (siehe Kapitel 5 auf Seite 48). Wenn das genannte Subsystem abgehängt ist, ist der Zugriff auf verschlüsselte Daten, die auf einem geschützten Laufwerk oder einem geschützten Wechseldatenträger gespeichert sind, nicht möglich. Betriebssysteme zeigen derartige Partitionen als nicht formatiert oder fehlerhaft an. Wenn auf dem Computer der System- oder Bootsektor der Festplatte geschützt ist, läßt der Systemkonfigurator das Trennen des Subsystems *Geschützte Laufwerke* nicht zu.
- Wir empfehlen Kaspersky KryptoStorage nicht auf Computern mit mehreren Betriebssystemen zu verwenden und dabei die Festplattenpartitionen zu verschlüsseln, die für die Ausführung der Betriebssysteme erforderlich sind.
- Die Systemdaten der geschützten logischen Partitionen und physischen Datenträger (physische Festplatten, Flash-Speicherkarten usw.) befinden sich im Stammverzeichnis der ersten Partition des physischen Datenträgers in der Datei `iwcs.bin`. Wenn die Partition mit der Datei `iwcs.bin` formatiert wird oder wenn die Datei `iwcs.bin` gelöscht, ersetzt oder beschädigt wird, ist der Zugriff auf die geschützten logischen Partitionen des physischen Datenträgers ggf. nicht möglich. Wenn auf dem Computer, auf dem Kaspersky KryptoStorage installiert ist, das Subsystem *Geschützte Laufwerke* (siehe Kapitel 5 auf Seite 48) ausgeführt wird, schützt das System die Datei `iwcs.bin` davor, gelöscht und geändert zu werden. Deshalb wird im Falle von geschützten Partitionen nicht empfohlen, das Subsystem *Geschützte Laufwerke* zu trennen. Wenn die Partition, in der die Datei `iwcs.bin` gespeichert ist, formatiert werden muß, entschlüsseln Sie alle Partitionen des physischen Datenträgers, führen die Formatierung durch und verschlüsseln die Partitionen anschließend erneut.

Beschränkungen bei der Verschlüsselung von logischen Festplattenpartitionen und Wechseldatenträgern:

- Die Verschlüsselung von logischen Festplattenpartitionen und Wechseldatenträgern ist möglich, solange die entsprechenden

Laufwerke eine Sektorgröße von 512 Byte aufweisen (standardmäßige Sektorgröße der meisten Laufwerke ähnlichen Typs).

- Die Verschlüsselung von dynamischen Partitionen wird nicht unterstützt.
- Es können nur lokale Laufwerke verschlüsselt werden. Die Verschlüsselung von Netzlaufwerken wird nicht unterstützt.
- Es ist nicht möglich, mehrere logische Partitionen auf einem physischen Laufwerk gleichzeitig zu verschlüsseln, zu entschlüsseln und anschließend erneut zu verschlüsseln. Jedoch können Sie die logischen Partitionen verschiedener Laufwerke gleichzeitig verwenden.
- Die Verschlüsselung der logischen Festplattenpartition, auf der Kaspersky KryptoStorage installiert ist, ist nur möglich, wenn es sich dabei um einen System- bzw. Bootsektor handelt.
- Die Verschlüsselung ist nur dann möglich, wenn die geschützte Partition nicht schreibgeschützt ist.
- Mit der Verschlüsselung eines Wechseldatenträgers kann nur dann begonnen werden, wenn der Wechseldatenträger von keinem Programm mehr verwendet wird. Während des Verschlüsselungsvorgangs kann der Wechseldatenträger weiterhin verwendet werden.
- Unter Windows 7 zeigt das Betriebssystem beim physischen Einbinden geschützter Wechseldatenträger die Meldung an, daß der Datenträger nicht formatiert ist und erst auf den Datenträger zugegriffen werden kann, nachdem er mit den Systemfunktionen eingebunden wurde (siehe Abschnitt 4.3.8 auf Seite 44).
- Die direkte Verschlüsselung von CDs/DVDs wird nicht unterstützt. CDs/DVDs können jedoch zum Speichern von geschützten Containern verwendet werden (siehe Abschnitt 4.2 auf Seite 28).

### **4.3.1. Besonderheiten bei der Verwendung von Programmen für die Arbeit mit Festplatten**

Einige Programme bieten die Möglichkeit, die Größe logischer Festplattenpartitionen zu ändern. Ändern Sie nicht die Größe logischer Festplattenpartitionen, die durch Kaspersky KryptoStorage geschützt sind. Dies kann zu Datenverlust führen.

Wenn es erforderlich sein sollte, eine derartige Operation auszuführen, entschlüsseln Sie die geschützten logischen Partitionen, führen die Umverteilung des freien Speicherplatzes durch und verschlüsseln sie diese anschließend wieder.

## 4.3.2. Verschlüsseln

### Wichtige Informationen!

Machen Sie sich zunächst mit den Besonderheiten beim Verschlüsseln von logischen Festplattenpartitionen und Wechseldatenträgern vertraut (siehe Abschnitt 4.2 auf Seite 287).

Das Verschlüsseln von logischen Festplattenpartitionen und Wechseldatenträgern erfolgt im Hintergrund. Deshalb können die Laufwerke während des Verschlüsselungsvorgangs weiterhin verwendet werden.

Falls erforderlich, kann der Verschlüsselungsvorgang unterbrochen werden (siehe Abschnitt 4.3.3 auf Seite 40). Danach besteht die Möglichkeit, den Verschlüsselungsvorgang fortzusetzen (siehe Abschnitt 4.3.4 auf Seite 41) oder den Vorgang ganz abzubrechen (siehe Abschnitt 4.3.5 auf Seite 41).

### Hinweis:

Der Übergang des Computers in den Standby-/Ruhemodus führt dazu, dass die Verschlüsselung automatisch unterbrochen wird. Nachdem der Computer den Standby-/Ruhemodus wieder verlassen hat, kann der Verschlüsselungsvorgang fortgesetzt oder ganz abgebrochen werden.

**So verschlüsseln Sie logische Festplattenpartitionen oder Wechseldatenträger:**

1. Führen Sie eine der folgenden Aktionen aus:
  - Wählen Sie im Explorer das Objekt (logische Festplattenpartition oder Wechseldatenträger) aus, das Sie verschlüsseln möchten. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Laufwerk verschlüsseln** aus.
  - Starten Sie die Anwendung Kaspersky KryptoStorage, indem Sie im Menü **Start** auf **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage** klicken. Klicken Sie in dem daraufhin angezeigte Fenster auf **Das Laufwerk verschlüsseln...**, wählen Sie die zu verschlüsselnde Partition aus und klicken Sie auf **OK**.

Daraufhin wird auf dem Bildschirm das Dialogfenster **Verschlüsseln des Laufwerks** angezeigt (siehe Abb. 8).



Abb. 8: Laufwerk verschlüsseln

2. Geben Sie in diesem Fenster die Parameter des zu verschlüsselnden Laufwerks an:
  - **Name des Laufwerks:** Geben Sie den Namen der zu verschlüsselnden Partition an. Sie können eine andere Partition auswählen, indem Sie auf **Durchsuchen...** klicken.
  - **Kennwort, Kennwort bestätigen, Kennworthinweis:** Geben Sie das Kennwort für den Zugriff auf das verschlüsselte Laufwerk und (optional) einen Kennworthinweis an. Diese Parameter werden für den Zugriff auf das Laufwerk verwendet.

**Hinweis:**

Empfehlungen zur Einrichtung des Kennworts und eines Kennworthinweises finden Sie in Abschnitt 1.4 auf Seite 8.

3. Klicken Sie auf **OK**, nachdem Sie alle erforderlichen Parameter angegeben haben.

Danach wird der Verschlüsselungsvorgang für das Objekt gestartet. Zu diesem Zeitpunkt wird das logische Laufwerk (der Wechseldatenträger) zu einem verschlüsselten Objekt.

**Wichtige Informationen!**

Wenn ein System- bzw. Bootsektor verschlüsselt wird, muß der Benutzer vor dem Starten des Betriebssystems autorisiert werden (für weitere Informationen siehe Abschnitt 4.3.7 auf Seite 43). Die Autorisierung ist nach jedem Neustart des Computers und auch nach dem Verlassen des Standby- oder Ruhezustands erforderlich.

## 4.3.3. Verschlüsselungsvorgang unterbrechen

Während des Verschlüsselungsvorgangs können Situationen auftreten, in denen es dringend erforderlich ist, den Vorgang zu unterbrechen, oder in denen der Schutz infolge einer außergewöhnlichen Situation (z.B. bei einem unerwarteten Herunterfahren des Computers) deaktiviert wird. In diesen Fällen kann der Verschlüsselungsvorgang zu einem späteren Zeitpunkt fortgesetzt werden.

**Wichtige Informationen!**

Das logische Laufwerk (Wechseldatenträger) ist unabhängig davon, ob der Verschlüsselungsvorgang vollständig oder teilweise durchgeführt wurde, ein verschlüsseltes Objekt. Deshalb ist die Verwendung dieses Laufwerks (Wechseldatenträgers) auch nach Unterbrechung des Verschlüsselungsvorgangs nur dann möglich, nachdem es eingebunden wurde (und die Autorisierung erfolgt ist). Wenn der Verschlüsselungsvorgang nicht abgeschlossen wurde, ist ein Teil der Daten auf der Partition unverschlüsselt.

**So unterbrechen Sie den Verschlüsselungsvorgang:**

1. Wählen Sie das Objekt aus, das Sie verschlüsseln möchten.
2. Führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie in dem angezeigten Dialogfenster auf **Abbrechen**, in dem der Fortschritt des Verschlüsselungsvorgangs angezeigt wird.
  - Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Verschlüsselungsvorgang abbrechen** aus.
3. Geben Sie in dem danach angezeigten Dialogfenster das **Kennwort** für den Zugriff auf das geschützte Objekt ein. Klicken Sie dann auf **OK**.

Daraufhin wird der Verschlüsselungsvorgang unterbrochen. Das geschützte Laufwerk (Wechsel Laufwerk) verbleibt im eingebundenen Zustand und kann weiterhin verwendet werden.

## 4.3.4. Verschlüsselungsvorgang fortsetzen

Ein zuverlässiger Schutz von Objekten ist nur dann sichergestellt, wenn der Verschlüsselungsvorgang vollständig abgeschlossen wurde. Wenn der Verschlüsselungsvorgang aus einem beliebigen Grund unterbrochen wurde, verbleibt ein Teil des Objekts unverschlüsselt. Der Verschlüsselungsvorgang kann mithilfe einer bestimmten Funktion fortgesetzt werden.

**So setzen Sie den Verschlüsselungsvorgang fort:**

1. Wählen Sie das Objekt aus, für das der Verschlüsselungsvorgang unterbrochen wurde.
2. Binden Sie das geschützte Objekt ein, wenn es nicht eingebunden ist (siehe Abschnitt 4.3.8 auf Seite 44).
3. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Laufwerksverschlüsselung fortsetzen** aus.
4. Geben Sie im danach angezeigten Dialogfenster das **Kennwort** für den Zugriff auf das geschützte Objekt ein. Klicken Sie dann auf **OK**.

Daraufhin wird der Verschlüsselungsvorgang fortgesetzt. Das geschützte Laufwerk (Wechsellaufwerk) verbleibt im eingebundenen Zustand und kann weiterhin verwendet werden.

## 4.3.5. Objekt in den unverschlüsselten Zustand zurücksetzen

Wenn die Verschlüsselung unterbrochen wurde, besteht die Möglichkeit, den Vorgang vollständig abzubrechen und das Objekt in den unverschlüsselten Zustand zurückzusetzen.

**So brechen Sie den Verschlüsselungsvorgang ab und setzen ein Objekt in den unverschlüsselten Zustand zurück:**

1. Wählen Sie das Objekt aus, für das der Verschlüsselungsvorgang unterbrochen wurde.

2. Binden Sie dieses Objekt ein, wenn es nicht eingebunden ist (siehe Abschnitt 4.3.8 auf Seite 44).
3. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Laufwerksverschlüsselung rückgängig machen** aus.
4. Geben Sie in dem daraufhin angezeigten Fenster das **Kennwort** des Besitzers des teilweise verschlüsselten Objekts an. Klicken Sie dann auf **OK**.

Danach wird der Prozeß zum Zurücksetzen des Objekts in den unverschlüsselten Zustand gestartet. Das geschützte Laufwerk (Wechseldatenträger) verbleibt im eingebundenen Zustand und kann weiterhin verwendet werden.

## 4.3.6. Objekt entschlüsseln

Sie können nur Objekte (logische Festplattenpartitionen und Wechseldatenträger) entschlüsseln, die eingebunden sind (für Informationen zum Einbinden von Objekten siehe Abschnitt 4.3.8 auf Seite 44).

### **Hinweis:**

Innerhalb eines physischen Laufwerks kann nur jeweils eine logische Partition gleichzeitig entschlüsselt werden. Wenn mehrere verschlüsselte logische Partitionen vorhanden sind, muß die Operation für jede Partition einzeln ausgeführt werden.

### **So entschlüsseln Sie Objekte:**

1. Wählen Sie das Objekt aus, das Sie entschlüsseln möchten.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Das Laufwerk entschlüsseln** aus.
3. Geben Sie in dem danach angezeigten Dialogfenster das **Kennwort** für den Zugriff auf das geschützte Objekt ein. Klicken Sie dann auf **OK**.

Das Entschlüsseln einer logischen Laufwerkspartition oder eines Wechseldatenträgers wird im Hintergrund ausgeführt. Deshalb können die Partitionen und Datenträger während der Entschlüsselung weiterhin verwendet werden.

Bei Bedarf kann der Entschlüsselungsvorgang unterbrochen werden. Die Unterbrechung des Entschlüsselungsvorgangs erfolgt analog zur Unterbrechung des Verschlüsselungsvorgangs (siehe Abschnitt 4.3.3 auf Seite 40).

Die Entschlüsselung kann zu einem späteren Zeitpunkt fortgesetzt werden. Dieser Vorgang wird analog zur Fortsetzung der Verschlüsselung ausgeführt (siehe Abschnitt 4.3.4 auf Seite 41).

Darüber hinaus besteht die Möglichkeit, die Entschlüsselung abzubrechen und zum vorherigen Zustand zurückzukehren. Das Abbrechen des Entschlüsselungsvorgangs erfolgt analog zum Abbrechen des Verschlüsselungsvorgangs (siehe Abschnitt 4.3.5 auf Seite 41). Nachdem Sie die Entschlüsselung abgebrochen haben, befindet sich das Objekt im teilweise verschlüsselten Zustand.

## 4.3.7. Bootvorgang von verschlüsseltem System- bzw. Bootlaufwerk ausführen

Wenn ein System- bzw. Bootlaufwerk durch Kaspersky KryptoStorage geschützt ist, kann das Betriebssystem, das auf dem Laufwerk installiert ist, erst gestartet werden, nachdem das Laufwerk eingebunden wurde. Dafür muß der jeweilige Benutzer vor dem Starten des Betriebssystems autorisiert werden.

### So binden Sie ein geschütztes System- bzw. Bootlaufwerk ein:

Geben Sie das **Kennwort** für den Zugriff auf die geschützte Partition ein.

#### Hinweis:

Wenn sich auf Ihrem Computer die System- und die Bootpartition auf unterschiedlichen logischen Laufwerken befinden und beide Partitionen geschützt sind, müssen beide Partitionen eingebunden werden.

Danach wird der Benutzer autorisiert. Bei erfolgreicher Autorisierung wird das Betriebssystem gestartet, das auf dem geschützten Laufwerk installiert ist.

#### Hinweis:

Wenn bei der Autorisierung ein falsches Kennwort eingegeben wurde, erscheint auf dem Bildschirm eine entsprechende Warnung. Danach wird der Kennwordhinweis angezeigt, wenn beim Anlegen des Kennworts ein Kennwordhinweis angegeben wurde. Sie können daraufhin erneut das Kennwort eingeben. Wenn kein Hinweis eingegeben wurde, können Sie den Autorisierungsvorgang erneut ausführen, indem Sie den Computer durch Drücken der Tastenkombination **STRG+ALT+ENTF** neu starten.

## 4.3.8. Geschützte logische Festplattenpartitionen und Wechseldatenträger einbinden

Die Verwendung (lesen, schreiben, umbenennen, kopieren, löschen usw.) von beliebigen geschützten logischen Partitionen ist nur dann möglich, wenn das Objekt eingebunden ist.

**So binden Sie eine logische Festplattenpartition oder einen Wechseldatenträger ein:**

1. Wählen Sie die geschützte Partition aus, die Sie einbinden möchten.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Laufwerk einbinden** aus.
3. Geben Sie in dem danach angezeigten Dialogfenster das Kennwort für den Zugriff auf die geschützte Partition ein. Klicken Sie dann auf **OK**.

Eingebundene Objekte sind nicht geschützt, sodaß alle Benutzer des jeweiligen Computers darauf zugreifen können. Deshalb ist es unerlässlich, geschützte Objekte sofort wieder zu trennen, nachdem Sie deren Verwendung abgeschlossen haben.

## 4.3.9. Geschützte logische Festplattenpartitionen und Wechseldatenträger trennen

Durch Trennen wird das geschützte Objekt wieder in einen Zustand versetzt, in dem es nicht bearbeitet werden kann, bis es wieder eingebunden wird.

### **Wichtige Informationen!**

Geschützte Partitionen dürfen erst getrennt werden, nachdem alle daran durchgeführten Änderungen gespeichert wurden.

### **So trennen Sie eine logische Festplattenpartition oder einen Wechseldatenträger:**

1. Wählen Sie das verschlüsselte Objekt (logische Festplattenpartition oder Wechseldatenträger) aus, dessen Verwendung abzuschließen ist.
2. Klicken Sie mit der rechten Maustaste auf die ausgewählte Datei bzw. den ausgewählten Ordner, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Laufwerk trennen** aus.

Wenn gleichzeitig mehrere verschlüsselte Objekte verwendet werden, nimmt das Trennen von allen Objekten eine gewisse Zeit in Anspruch. Es können jedoch auch besondere Situationen auftreten, in denen es erforderlich ist, alle verschlüsselten Objekte gleichzeitig zu trennen. Hierfür können Sie einen Neustart des Computers ausführen (nachdem Sie alle durchgeführten Änderungen gespeichert haben). Nach dem Neustart des Computers sind alle verschlüsselten Objekte getrennt.

## **4.3.10. Laufwerke wiederherstellen**

### **Wichtige Informationen!**

Für die Verwendung der Funktionen zur Wiederherstellung von Laufwerken ist es erforderlich, daß Sie auf dem Computer über die Rechte des lokalen Administrators verfügen.

Aus dem Fenster der Anwendung Kaspersky KryptoStorage können Sie die Funktion aufrufen, mit der Sie Speicherplatz auf der Festplatte, auf Flash-Speicherkarten und auf anderen USB-Datenspeichergeräten freigegeben können, der durch geschützte Partitionen belegt ist, wenn der Zugriff darauf nicht mehr möglich ist.

Die Anforderung zum Löschen von Informationen über eine verschlüsselte Partition ohne deren Entschlüsselung kann in den folgenden Situationen auftreten:

- Verlust eines Schlüssels für den Zugriff auf eine geschützte Partition, wodurch das Einbinden oder Entschlüsseln der Partition nicht mehr möglich ist.

- Die geschützte Partition wurde ohne Kaspersky KryptoStorage und dem Subsystem für geschützte logische Laufwerke formatiert. Folglich sind alle Daten dieser Partition verloren, aber auf dem Laufwerk sind Systemdaten über das Vorhandensein der Partition gespeichert. Auf diese Partition können Sie auf einem Computer mit Kaspersky KryptoStorage und dem gestarteten Subsystem *Geschützte logische Laufwerke* nur zugreifen, nachdem Sie die Informationen über die Entschlüsselung gelöscht haben. Der Zugriff kann möglicherweise dann erforderlich sein, wenn nach der Formatierung unverschlüsselte Daten auf der Partition gespeichert wurden.
- Wenn die Größe der geschützten Partition geändert wurde (siehe Abschnitt 4.3.1 auf Seite 37). Dadurch tritt ein Konflikt zwischen der durch das System berechneten Größe und der realen Größe der geschützten Partition auf.

Wenn auf dem Computer, auf dem Kaspersky KryptoStorage installiert ist, das Subsystem *Geschützte Laufwerke* (siehe Kapitel 5 auf Seite 48) ausgeführt wird, ist der Zugriff auf die oben angegebenen geschützten Partitionen des Laufwerks nicht möglich. Darüber hinaus kann der Speicherplatz, der von den Partitionen auf dem Laufwerk eingenommen wird, nicht verwendet werden. Mithilfe der Funktionen zum Wiederherstellen von Laufwerken kann dieser Speicherplatz wieder für die Verwendung freigegeben werden, auch für die Verwendung durch Kaspersky KryptoStorage.

Vor Verwendung der Wiederherstellungsfunktionen müssen die folgenden Aktionen ausgeführt werden:

1. Schließen Sie alle Operationen ab, die mit dem Verschlüsseln, Umschlüsseln und Entschlüsseln auf allen Partitionen des physischen Laufwerks verbunden sind.
2. Trennen sie die geschützten Partitionen des physischen Laufwerks ab, deren Informationen mithilfe der Wiederherstellungsfunktionen aus dem System gelöscht werden müssen.

### **Wichtige Informationen!**

Gehen Sie bei der Auswahl der geschützten Partitionen sorgfältig vor. Nach dem Löschen der Systeminformationen über die geschützte Partition können auf dem Laufwerk keine Daten aus dieser Partition mehr entschlüsselt werden. Deshalb wird die Partition, wenn sie verschlüsselt war, als unformatiert angezeigt.

**So geben Sie Speicherplatz, der von einer geschützten Partition eingenommen wird, auf einem Laufwerk zur Verwendung frei:**

1. Starten Sie die Anwendung Kaspersky KryptoStorage. Klicken Sie dazu im Menü **Start** auf **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**.

2. Klicken Sie im Fenster der Steuerung von Kaspersky KryptoStorage auf **Laufwerkswiederherstellung**.
3. Wählen Sie im Fenster **Laufwerkswiederherstellung** die geschützte Partition aus, deren Systemangaben vom Laufwerk gelöscht werden müssen. Klicken Sie anschließend mit der rechten Maustaste auf die Partition und wählen in dem daraufhin angezeigten Kontextmenü die Option **Information über das verschlüsselte Gebiet löschen** aus.

## 4.4. Sicheres Löschen von geschützten und ungeschützten Objekten

Dateien und Ordner, die mit gewöhnlichen Methoden gelöscht wurden, können danach möglicherweise mithilfe spezieller Programme wiederhergestellt werden. Folglich können dritte Personen auf die Informationen zugreifen, die in den gelöschten Objekten gespeichert waren. Dieses Problem kann durch das sichere Löschen von Objekten gelöst werden.

Die Funktionen zum sicheren Löschen können sowohl für geschützte als auch für ungeschützte Objekte ausgeführt werden.

### **Wichtige Informationen!**

Beim sicheren Löschen von Ordnern werden alle Dateien in allen Unterordnern und alle Unterordner gelöscht

Ordner, die verschlüsselt sind, können nur sicher gelöscht werden, wenn sie eingebunden sind.

Das sichere Löschen von geschützten Containern ist nur möglich, wenn die Container getrennt sind.

**So löschen Sie Dateien und Ordner sicher, sodass sie hinterher nicht wiederhergestellt werden können:**

1. Wählen Sie das Objekt (Datei, Ordner oder geschützten Container) aus, das Sie löschen möchten.
2. Klicken Sie mit der rechten Maustaste auf das ausgewählte Objekt, und wählen Sie in dem daraufhin angezeigten Kontextmenü die Option **Kaspersky KryptoStorage ► Sicher löschen** aus.
3. Klicken Sie in dem daraufhin angezeigten Fenster auf **Ja**.

# KAPITEL 5. SUBSYSTEME KONFIGURIEREN

Kaspersky KryptoStorage umfaßt drei Subsysteme, mit denen jeweils ein bestimmter Objekttyp verschlüsselt werden kann. Die Bezeichnungen dieser Subsysteme können der folgenden Tabelle entnommen werden.

Subsystem	Bedeutung
Geschützte Laufwerke	Für die Verschlüsselung von logischen Festplattenpartitionen und Wechseldatenträgern
Geschützte Container	Zum Erstellen und Verwenden von geschützten Containern
Geschützte Ordner	Zum Erstellen und Verwenden von geschützten Ordnern

Die in Kaspersky KryptoStorage enthaltenen Subsysteme können über die Steuerung von **Kaspersky KryptoStorage** eingerichtet werden.

Um die Steuerung von **Kaspersky KryptoStorage** aufzurufen, klicken Sie im Menü **Start** auf **Alle Programme ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**.

Daraufhin wird auf dem Bildschirm das Fenster der Anwendung angezeigt, in dem Sie die Informationen über die Subsysteme von Kaspersky KryptoStorage prüfen können, die auf Ihrem Computer installiert sind (siehe Abb. 9).

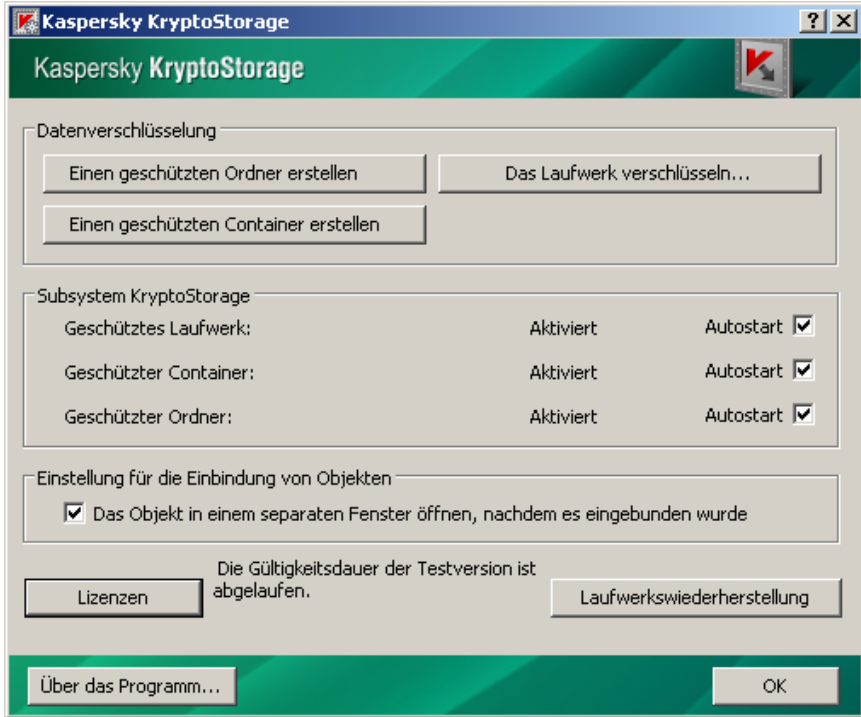


Abb. 9: Kaspersky KryptoStorage-Subsysteme konfigurieren

Rechts von den Bezeichnungen der einzelnen Subsysteme befindet sich das Kontrollkästchen **Autostart**. Durch Aktivieren dieses Kontrollkästchens wird das Subsystem automatisch gestartet.

Nach der Installation von Kaspersky KryptoStorage ist für alle Subsysteme aktiviert, daß sie automatisch gestartet werden. Die Einstellung des Parameters für das automatische Starten von Subsystemen kann jedoch geändert werden:

- Durch Deaktivieren des Kontrollkästchens **Autostart** werden Subsysteme nicht mehr automatisch gestartet.
- Durch Aktivieren des Kontrollkästchens **Autostart** werden Subsysteme automatisch gestartet.

**Hinweis:**

Änderungen der Einstellungen zum automatischen Starten von Subsystemen werden erst nach einem Neustart des Computers wirksam.

Beim Deaktivieren der Autostartfunktion für ein Subsystem müssen die Besonderheiten der Ausführung von Kaspersky KryptoStorage-Subsystemen berücksichtigt werden. In der Tabelle unten sind die Folgen des Deaktivierens für jedes Subsystem aufgeführt.

Subsystem	Folgen des Deaktivierens des Subsystems
Geschützte Laufwerke	<p>Das Betriebssystem identifiziert geschützte Laufwerke als unformatiert. Der Inhalt ist verschlüsselt.</p> <p>Auf die Systemfunktionen zur Verwendung von logischen Festplattenpartitionen und Wechseldatenträgern kann nicht zugegriffen werden.</p> <p><b>Hinweis:</b> Das Deaktivieren des Subsystems bei einer geschützten System- bzw. Bootpartition ist nicht möglich.</p>
Geschützte Container	<p>Der Zugriff auf den Inhalt von geschützten Containern ist nicht möglich. Der Inhalt ist verschlüsselt.</p> <p>Auf die Systemfunktionen zur Verwendung von geschützten Containern kann nicht zugegriffen werden.</p>
Geschützte Ordner	<p>Die darin enthaltenen geschützten Ordner und Dateien können von jedem beliebigen Benutzer vom Computer gelöscht werden.</p> <p>Die enthaltenen Dateien sind verschlüsselt, nur die Unterordnerstruktur kann angezeigt werden.</p> <p>Auf die Systemfunktionen zur Verwendung von geschützten Dateien und Ordnern kann nicht zugegriffen werden.</p>

# KAPITEL 6. KASPERSKY KRYPTOSTORAGE DEINSTALLIEREN

Für geschützte Objekte entspricht das Deinstallieren von Kaspersky KryptoStorage dem Deaktivieren von allen Subsystemen (siehe Kapitel 5 auf Seite 48:

- Die darin enthaltenen geschützten Ordner und Dateien können von jedem beliebigen Benutzer vom Computer gelöscht werden. Die enthaltenen Dateien sind verschlüsselt, nur die Unterordnerstruktur kann angezeigt werden.
- Container befinden sich weiterhin im geschützten Zustand, sie können jedoch nicht verwendet werden, da sie nicht eingebunden werden können.
- Die Verschlüsselung von logischen Festplattenpartitionen und Wechseldatenträgern bleibt erhalten. Der Zugriff auf die Daten, die auf diesen Laufwerken gespeichert sind, ist jedoch nicht möglich, da sie nicht eingebunden werden können.

## **Wichtige Informationen!**

Im Betriebssystem gelten derartige Objekte als unformatiert. Deshalb wird beim Zugriffsversuch auf ein geschütztes Objekt vorgeschlagen, das Objekt zu formatieren. Durch das Formatieren des Objekts gehen alle Daten verloren. Deshalb darf die Formatierung nicht durchgeführt werden, wenn das Objekt für Sie wichtige Daten enthält.

Das Deinstallieren des Programms ist nicht möglich, wenn die System- bzw. Bootpartition der Festplatte geschützt ist. Deshalb ist in diesem Fall das Starten des Betriebssystems und folglich das Zugreifen auf die auf dem Laufwerk gespeicherten Daten nicht möglich.

Vor dem Deinstallieren des Systems müssen die folgenden vorbereitenden Aktionen ausgeführt werden:

- Entschlüsseln von System- bzw. Bootpartitionen und anderer logischer Laufwerke und Wechseldatenträger

- Einbinden geschützter Container und Ordner und Kopieren des Inhalts in ungeschützte Ordner auf ungeschützten Festplatten oder Wechseldatenträgern

**Wichtige Informationen!**

Für die Deinstallation von Kaspersky KryptoStorage muß der Benutzer über lokale Administratorrechte auf dem Computer verfügen.

Für die Deinstallation von Kaspersky KryptoStorage werden die Standardfunktionen von Microsoft Windows verwendet.

**So deinstallieren Sie Kaspersky KryptoStorage:**

1. Öffnen Sie das Fenster **Software**. Klicken Sie dafür im Menü **Start** auf **Einstellungen** ► **Systemsteuerung**. Klicken Sie im Fenster der Systemsteuerung zweimal auf **Software**.
2. Wählen Sie im Fenster **Software** die Anwendung **Kaspersky KryptoStorage** aus, und klicken Sie auf **Löschen**.

Führen Sie zum Abschluß der Deinstallation des Systems einen Neustart des Computers durch.

# APPENDIX A. GLOSSAR

## **Kaspersky KryptoStorage**

System, das für den kryptografischen Schutz vertraulicher Informationen, die auf dem Computer des Benutzers gespeichert sind, konzipiert ist, sodass der unerlaubte Zugriff darauf nicht mehr möglich ist.

## **Sicheres Löschen eines Objekts**

Funktion zum Löschen von Dateien und Ordnern, sodass nicht nur der Name des Objekts aus dem Dateisystem gelöscht wird, sondern auch der Inhalt des zu löschenden Objekts entfernt wird.

## **Informationen schützen**

Methoden zum Einschränken des Zugriffs auf Informationen von Benutzern (Benutzerkategorien).

## **Geschützter Container**

Datei mit einem bestimmten Format, die vom System als virtuelles logisches Laufwerk angesehen wird. Die eigentlichen Daten sind in einer Datei gespeichert.

## **Geschütztes Objekt**

Unter geschützten Objekten sind beliebige Objekte zu verstehen, die zum Speichern von Daten vorgesehen sind, die von Kaspersky KryptoStorage verschlüsselt wurden.

## **Vertrauliche Daten**

Daten, auf die der Zugriff beschränkt ist. Auf vertrauliche Daten können nur die Benutzer zugreifen, die für den Zugriff definiert sind.

## **Kennwort**

Zeichenfolge, die für den Zugriff auf den Inhalt geschützter Objekte verwendet wird. Benutzer sollten ihre Kennwörter geheim halten.

**Transparente Verschlüsselung**

Mechanismus, mit dem Daten in einem geschützten Objekt ausschließlich in verschlüsselter Form gespeichert werden. Die Arbeit in dem geschützten Objekt erfolgt so, daß die Daten beim Zugriff darauf automatisch im Arbeitsspeicher entschlüsselt und beim Speichern wieder verschlüsselt werden.

# APPENDIX B. REFERENZINFORMATIONEN

## B.1. Kaspersky Lab

Kaspersky Lab wurde 1997 von Eugene Kaspersky gegründet und befindet sich bis heute in Privatbesitz. Das Unternehmen mit Hauptsitz in Moskau beschäftigt weltweit über 1.300 hochspezialisierte Mitarbeiter, davon mehr als 130 in der deutschen Niederlassung in Ingolstadt. Rund um den Globus entwickeln die Viren-Experten seit Jahren zuverlässige, innovative IT-Sicherheitslösungen zum Schutz vor Viren, Hackern und Spam.

Für den bestmöglichen Schutz forscht Kaspersky Lab ständig an neuen Technologien und ist dabei ein wichtiger Wegbereiter für neue Sicherheitsstandards. So hat Kaspersky Lab als erster Hersteller auf einen proaktiven Schutz vor unbekanntem Viren gesetzt, sondern auch den ersten Virenschutz für Linux entwickelt sowie die erste Antiviren Lösung mit Citrix-Zertifikat auf den Markt gebracht.

Die Produkte und Services schützen 250 Millionen Anwender auf der ganzen Welt. Zu den Kunden zählen eine Vielzahl internationaler Firmen und Institutionen.

Anschrift:	Kaspersky Lab, Steinheilstrasse 13, D-85053 Ingolstadt, Deutschland
Technischer Support:	<a href="http://support.kaspersky.com/de/">http://support.kaspersky.com/de/</a>
Webforum von Kaspersky Lab:	<a href="http://www.kaspersky.de/forum">www.kaspersky.de/forum</a>
Antiviren-Labor:	<a href="mailto:newvirus@kaspersky.com">newvirus@kaspersky.com</a> (nur zum Einsenden neuer Viren, die zuvor in ein Archiv gepackt wurden)
Abteilung für Handbücher und Hilfesysteme:	<a href="mailto:docfeedback@kaspersky.de">docfeedback@kaspersky.de</a> (Diese Adresse ist ausschließlich für Rückmeldungen über Handbücher und elektronische Hilfesysteme gedacht – hierüber kann leider kein Support geleistet werden.)

Allgemeine Informationen:	<a href="http://www.kaspersky.de/kontakt">www.kaspersky.de/kontakt</a>
Internet:	<a href="http://www.kaspersky.de">www.kaspersky.de</a> <a href="http://www.viruslist.de">www.viruslist.de</a>

## B.2. Lizenz für die Bibliothek Windows Installer XML (WiX)

Diesem Anhang können Sie den Text der Lizenz für die Bibliothek Windows Installer XML (WiX) 2.0 Copyright (c) 2005-2008 Microsoft Corporation entnehmen.

### Hinweis:

Den Lizenztext finden Sie auch unter:  
<http://www.opensource.org/licenses/cpl1.0.php>.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLICLICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAMCONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

### 1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
  - i) changes to the Program, and
  - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

## 2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

## 3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

#### 4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

## 5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

## 6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## 7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.