



## Was ist PGP Desktop?

PGP Desktop bietet umfassende Sicherheit für Desktops und Laptops und ermöglicht den Schutz vertraulicher Daten von Unternehmen, Arbeitsgruppen und Privatpersonen, ohne Änderungen an der bestehenden IT-Infrastruktur vorzunehmen oder Arbeitsprozesse zu stören. Diese ausgezeichnete, benutzerfreundliche Lösung verschlüsselt E-Mails, Dateien, virtuelle Laufwerke und ganze Festplatten mit einer einzigen Desktopanwendung.

Die Anwendungen der PGP Desktop-Familie wurde zu mehreren Produktbündeln zusammengestellt.

- **PGP Desktop Professional 9.6** enthält PGP Desktop Email und PGP Whole Disk Encryption.
- **PGP Desktop Storage 9.6** enthält PGP Whole Disk Encryption und PGP NetShare.
- **PGP Desktop Enterprise 9.6** enthält PGP Desktop Email, PGP Whole Disk Encryption und PGP NetShare.

## PGP Desktop Email

Mit PGP Desktop Email können Sie E-Mail-Nachrichten automatisch und transparent gemäß von Administratoren für Sie definierten Richtlinien oder, falls Sie nicht in einer mit PGP Universal verwalteten Umgebung arbeiten, gemäß von Ihnen selbst gesteuerten Richtlinien verschlüsseln, signieren, entschlüsseln und verifizieren.

## PGP NetShare

Sie können mit PGP NetShare berechtigten Anwendern die Freigabe geschützter Dateien in einem freigegebenen Speicherbereich ermöglichen, z. B. auf einem Dateiserver, in einem freigegebenen Ordner oder auf einem USB-Wechsellaufwerk.

Darüber hinaus können Sie mit PGP Desktop folgende Aufgaben ausführen:

- Einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit eigenem Laufwerksbuchstaben verwenden.
- Geschützte Zip-Archive erstellen.
- Dateien und Ordner in einem einzelnen, verschlüsselten und komprimierten Paket ablegen, das auch auf Windows-Systemen geöffnet werden kann, auf denen PGP Desktop nicht installiert ist.

## Neu bei PGP Desktop?

Dieses Handbuch mit schrittweisen Anleitungen hilft Ihnen beim Einstieg. Sie werden schnell feststellen, dass Sie Ihre Daten mit PGP Desktop so einfach schützen können, als würden Sie einen Schlüssel im Schloss umdrehen.

- Dieser *Schnelleinstieg* unterstützt Sie bei der Installation von PGP Desktop.
- Das *PGP Desktop Anwenderhandbuch* enthält ausführlichere Informationen über PGP Desktop. In diesem Handbuch wird der Begriff des Schlüsselpaars erläutert, Sie erfahren, warum Sie ein Schlüsselpaar erstellen sollten, wie Sie es erstellen und wie Sie Schlüssel mit anderen austauschen, um Ihre eigenen Daten zu verschlüsseln und Daten sicher mit anderen auszutauschen.

## PGP Whole Disk Encryption

Sie können mit PGP Whole Disk Encryption (WDE) den ganzen Inhalt Ihres Systems oder eines von Ihnen angegebenen externen Laufwerks bzw. USB-Flash-Laufwerks sperren.

### Inhalt

■ <a href="#">Was ist PGP Desktop?</a>	1
■ <a href="#">Was wird installiert?</a>	2
■ <a href="#">Die Grundlagen</a>	3
■ <a href="#">PGP Desktop installieren</a>	4
■ <a href="#">PGP Desktop starten</a>	4
■ <a href="#">Der PGP Desktop-Hauptbildschirm</a>	5
■ <a href="#">PGP Desktop Email verwenden</a>	6
■ <a href="#">Wurde meine Nachricht verschlüsselt?</a>	7
■ <a href="#">PGP NetShare verwenden</a>	8
■ <a href="#">PGP Virtual Disk-Laufwerke erstellen</a>	9
■ <a href="#">PGP WDE - Bewährte Methoden</a>	10
■ <a href="#">Laufwerk mit PGP WDE verschlüsseln</a>	12
■ <a href="#">PGP Zip-Archive erstellen</a>	13
■ <a href="#">Dateien sicher löschen</a>	16
■ <a href="#">Freien Speicherplatz sicher löschen</a>	17
■ <a href="#">Weitere Informationen</a>	18

## Verwendete Symbole



**Hinweis**



**Achtung**

- Dateien und Ordner vollständig zerstören, so dass sie auf keine Weise wiederhergestellt werden können.
- Freien Speicherplatz auf Laufwerken sicher löschen, so dass die gelöschten Daten keinesfalls wiederhergestellt werden können.

- Informationen zur Implementierung, Verwaltung und Richtliniendurchsetzung mit PGP Desktop finden Sie im *PGP Universal Administrator-Handbuch*.

## Systemanforderungen

- Windows Vista, Windows XP (SP 1 oder 2), Windows 2000 (SP 4) und Windows 2003 Server (SP 1)  
(PGP WDE wird unter Windows 2000 und Windows 2003 Server nicht unterstützt.)
- 128 MB RAM (256 MB empfohlen)
- 64 MB Festplattenspeicher

---

## Was wird installiert?

Der Zugriff auf die erworbenen Funktionen von PGP Desktop erfolgt mit Hilfe von Lizenzen. Je nach Lizenz sind einige oder alle Anwendungen der PGP Desktop-Anwendungsfamilie aktiv.

Dieses Dokument enthält Anweisungen für die Anzeige der mit Ihrer Lizenz aktivierten Funktionen.



**PGP Desktop Email** ist ein Mitglied der PGP Desktop-Anwendungsfamilie. Mit PGP Desktop Email können Sie E-Mail-Nachrichten durch von Ihnen kontrollierte Richtlinien automatisch und transparent verschlüsseln, signieren, entschlüsseln und überprüfen. Außerdem können Sie mit PGP Desktop Email Instant Messaging-Sitzungen für Clients wie AIM und iChat verschlüsseln. Bei beiden Benutzern muss PGP Desktop Email aktiviert sein.



**PGP NetShare** ist ein Mitglied der PGP Desktop-Anwendungsfamilie. Mit PGP NetShare können Sie Anwendern die gemeinsame Verwendung geschützter Dateien in einem freigegebenen Speicherbereich ermöglichen, z. B. auf einem firmeninternen Dateiserver, in einem freigegebenen Ordner oder auf einem Wechseldatenträger (z. B. einem USB-Laufwerk). Die verschlüsselten Dateien im geschützten Ordner werden den berechtigten Anwendern weiterhin als normale Anwendungsdateien angezeigt. Jeder mit physischem Zugriff auf die Dateien kann sie sehen, aber nicht verwenden.



**PGP Whole Disk Encryption (WDE)** ist ein Mitglied der PGP Desktop-Anwendungsfamilie. Sie können mit PGP WDE den ganzen Inhalt Ihres Systems oder eines von Ihnen angegebenen externen Laufwerks bzw. USB-Flash-Laufwerks sperren. Bootsektoren, Systemdateien und Auslagerungsdateien werden dabei ebenfalls verschlüsselt. Wenn Sie Ihr Boot-Laufwerk mit PGP Whole Disk Encryption verschlüsseln, müssen Sie sich im Fall des Verlusts oder Diebstahls Ihres Computers keine Sorgen machen: Der Zugriff auf Ihre Daten ist nur mit dem korrekten Passwort möglich.

In PGP Desktop Email sind die folgenden weiteren Komponenten von PGP Desktop enthalten:



**PGP Virtual Disk-Laufwerke:** Verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit eigenem Laufwerksbuchstaben. Sie können weitere Anwender für ein Laufwerk erstellen und dadurch den autorisierten Personen den Zugriff gestatten. Ein PGP Virtual Disk-Laufwerk eignet sich ideal als Speicherort für vertrauliche Dateien: Es ist so sicher wie ein Tresor. Nur wenn die Türen des Tresors geöffnet sind (wenn das Laufwerk aktiviert ist), können die darin gespeicherten Dateien geändert oder entfernt bzw. zusätzliche Dateien hinzugefügt werden. Andernfalls (wenn das Laufwerk deaktiviert ist) sind alle Daten auf dem Laufwerk geschützt.



**PGP Zip:** Fügt beliebige Kombinationen von Dateien und Ordnern in ein verschlüsseltes, komprimiertes, portables Archiv ein. PGP Desktop muss auf dem System installiert sein, um ein PGP Zip-Archiv erstellen oder öffnen zu können. PGP Zip ist ein Tool für die sichere Archivierung vertraulicher Daten und eignet sich sowohl für deren Weitergabe an andere als auch für die Sicherung.

**Selbstentschlüsselnde PGP-Archive (SDAs):** Dateien und Ordner werden in einem verschlüsselten und komprimierten Paket abgelegt, das auch auf Windows-Systemen geöffnet werden kann, auf denen PGP Messaging oder PGP Desktop nicht installiert ist. Selbstentschlüsselnde Archive sind die ideale Lösung für den sicheren Austausch von Dateien mit Personen, die keine PGP-Software installiert haben.



**PGP Shredder:** Dateien und Ordner werden vollständig zerstört, so dass sie selbst mit Datenwiederherstellungssoftware nicht wiederhergestellt werden können. Beim Löschen einer Datei mit dem Papierkorb in Windows wird sie nicht wirklich gelöscht, sondern bleibt auf der Festplatte, bis sie schließlich überschrieben wird. Bis zu diesem Zeitpunkt kann sie von einem Angreifer ohne großen Aufwand wiederhergestellt werden. PGP Shred überschreibt Dateien hingegen sofort mehrmals. Diese Vorgehensweise ist so wirkungsvoll, dass diese Dateien selbst mit der besten Festplattenwiederherstellungssoftware nicht wiederhergestellt werden können. Freier Speicherplatz auf Laufwerken wird ebenfalls absolut sicher gelöscht, so dass gelöschte Daten keinesfalls wiederhergestellt werden können.



**Schlüsselverwaltung:** PGP Messaging verwaltet auch PGP-Schlüssel, und zwar sowohl Ihre eigenen Schlüsselpaare als auch die öffentlichen Schlüssel anderer. Mit Ihrem privaten Schlüssel entschlüsseln Sie Nachrichten, die mit Ihrem öffentlichen Schlüssel verschlüsselt wurden. Außerdem schützen Sie damit Ihre PGP Virtual Disk-Laufwerke. Mit öffentlichen Schlüsseln verschlüsseln Sie Nachrichten an andere oder fügen Sie Benutzer zu PGP Virtual Disk-Laufwerken hinzu.

## Die Grundlagen

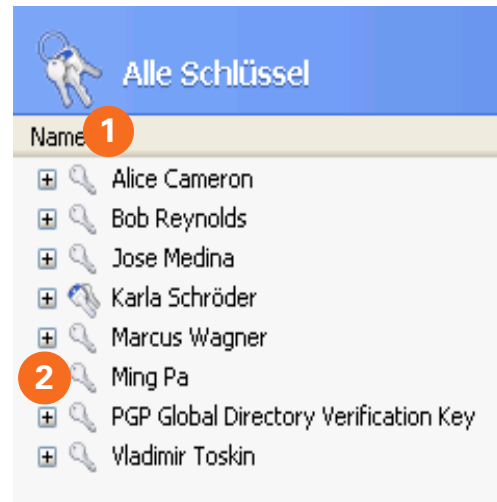
PGP Desktop verwendet Schlüssel, um Ihre Nachrichten zu verschlüsseln, zu signieren, zu entschlüsseln und zu überprüfen.

Nach der Installation von PGP Desktop werden Sie aufgefordert, ein PGP-Schlüsselpaar zu erstellen. Ein Schlüsselpaar ist eine Kombination von privatem und öffentlichem Schlüssel.

- Der **private Schlüssel** und das zugehörige Passwort müssen, wie schon der Name sagt, unter Verschluss gehalten werden. Falls jemand in Besitz Ihres privaten Schlüssels und Ihres Passworts gelangt, kann diese Person Ihre Nachrichten lesen und sich anderen gegenüber als Sie ausgeben. Mit dem privaten Schlüssel werden eingehende verschlüsselte Nachrichten entschlüsselt und ausgehende Nachrichten signiert.
- Ihren **öffentlichen Schlüssel** können Sie beliebig weitergeben. Es gibt dazu kein Passwort. Mit dem öffentlichen Schlüssel werden Nachrichten so verschlüsselt, dass sie nur mit Ihrem privaten Schlüssel entschlüsselt werden können. Außerdem werden damit von Ihnen signierte Nachrichten verifiziert.

In Ihrem Schlüsselbund befinden sich sowohl Ihre eigenen Schlüsselpaare als auch die öffentlichen Schlüssel anderer Anwender. Sie verwenden diese öffentlichen Schlüssel, um ihren Besitzern verschlüsselte Nachrichten zu senden. Klicken Sie auf das Bedienfeld **PGP Keys**, um die Schlüssel in Ihrem Schlüsselbund anzuzeigen:

- 1 Das Symbol für ein PGP-Schlüsselpaar zeigt zwei Schlüssel: je einen für den privaten und den öffentlichen Schlüssel. In der Abbildung verfügt beispielsweise Alice Cameron über ein PGP-Schlüsselpaar.
- 2 Die Symbole für die öffentlichen Schlüssel anderer Anwender enthalten nur einen Schlüssel. Der öffentliche Schlüssel von Ming Pa wurde beispielsweise dem Schlüsselbund hinzugefügt (siehe Abbildung).



## PGP Desktop installieren

Für die Installation ist ein Neustart des Systems erforderlich.

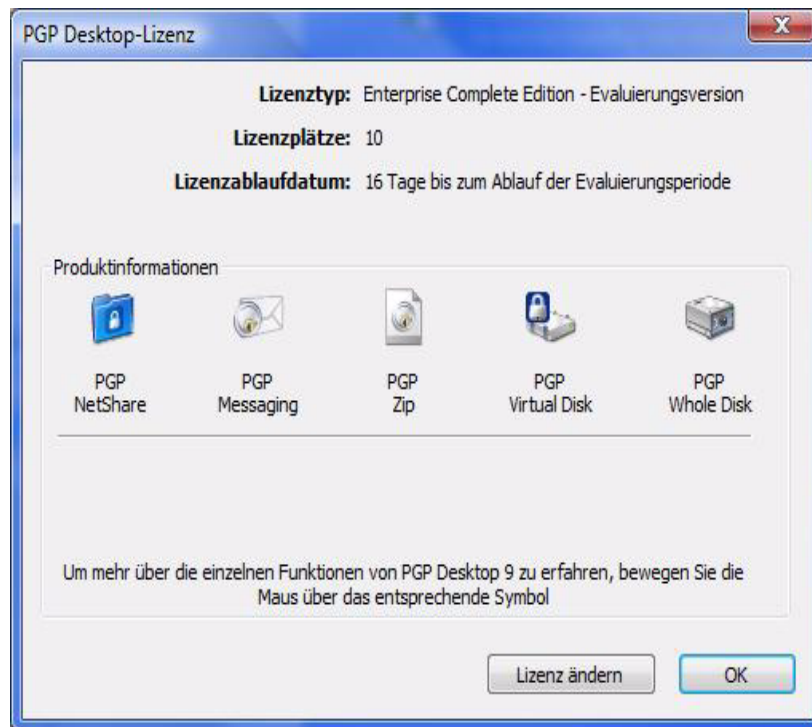
Die PGP Corporation empfiehlt, alle geöffneten Anwendungen vor Beginn der Installation zu beenden.



Wenn Sie PGP Desktop in einer mit PGP Universal verwalteten Umgebung verwenden, ist das Installationsprogramm von PGP Desktop möglicherweise mit spezifischen Funktionen und/oder Einstellungen konfiguriert.

So installieren Sie PGP Desktop:

- 1 Navigieren Sie zum Installationsprogramm für PGP Messaging.  
Möglicherweise wurde das Installationsprogramm von Ihrem PGP-Administrator mit dem Bereitstellungstool Microsoft SMS verteilt.
- 2 Doppelklicken Sie auf das Installationsprogramm.
- 3 Folgen Sie den Anweisungen auf dem Bildschirm.
- 4 Starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden.
- 5 Folgen Sie nach dem Neustart den Anweisungen am Bildschirm zur Konfiguration von PGP Desktop.



Wenn Sie sehen möchten, welche Funktionen Ihre PGP-Lizenz unterstützt, öffnen Sie PGP Desktop und klicken im Menü **Hilfe** auf **Lizenz**. Funktionen mit einem grünen Häkchen werden von der aktiven Lizenz unterstützt. In der Abbildung werden PGP Desktop, PGP Zip und PGP Virtual Disk unterstützt.

## PGP Desktop starten

Sie können PGP Desktop auf folgende Arten starten:

- Doppelklicken Sie auf das Symbol **PGP Tray**.
- Klicken Sie mit der rechten Maustaste auf das Symbol **PGP Tray**, und wählen Sie **PGP Desktop öffnen** aus.
- Klicken Sie im Menü **Start** auf **Programme > PGP > PGP Desktop**.



PGP Tray-Symbol

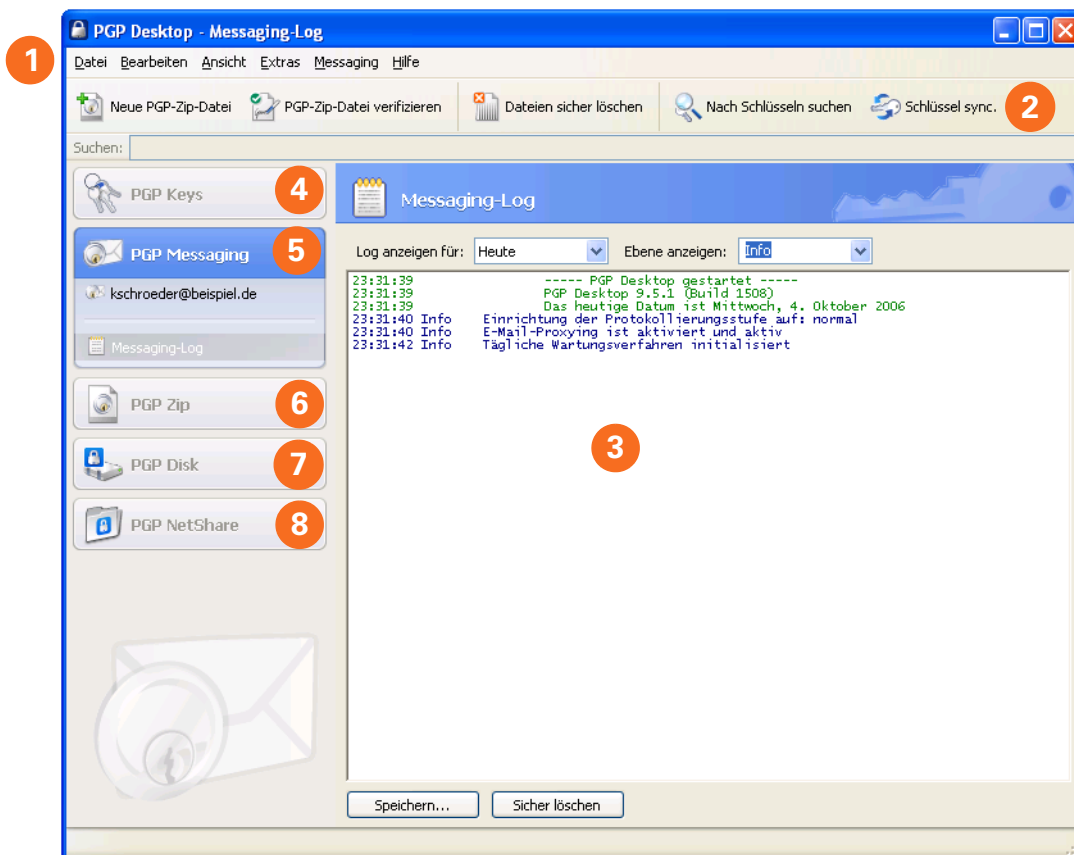
# Der PGP Desktop-Hauptbildschirm

Über den PGP Desktop-Hauptbildschirm können Sie einfach auf alle Funktionen zugreifen.



Je nach Lizenz verfügen Sie möglicherweise über keine Zugriffsberechtigung für bestimmte Komponenten von PGP Desktop.

- 1 PGP-Menüleiste:** Ermöglicht über seine Menüs und Befehle den Zugriff auf alle PGP Desktop-Funktionen.
- 2 PGP-Symbolleiste:** Ermöglicht den Zugriff auf die gängigsten Aufgaben mit PGP Desktop.
- 3 Arbeitsbereich:** Im **Arbeitsbereich** konfigurieren Sie die Einstellungen für die aktive Funktion. Die Abbildung zeigt den PGP Desktop Email-Arbeitsbereich mit aktiviertem Messaging-Protokoll.



- 4 Bedienfeld „PGP Keys“:** Dient zur Kontrolle Ihrer PGP-Schlüssel.
- 5 Bedienfeld „PGP Messaging“:** Dient zur Steuerung von PGP Desktop Email.
- 6 Bedienfeld „PGP Zip“:** Dient zur Steuerung von PGP Zip-Archiven.
- 7 Bedienfeld „PGP Disk“:** Dient zur Steuerung von PGP Virtual Disk-Laufwerken und von mit PGP Whole Disk verschlüsselten Laufwerken.
- 8 PGP NetShare:** Dient zur Steuerung von PGP NetShare.

## PGP Desktop Email verwenden

PGP Desktop Email verschlüsselt und signiert automatisch und transparent ausgehende Nachrichten und entschlüsselt und verifiziert eingehende Nachrichten. Sie können Ihre E-Mails einfach wie immer senden und empfangen. Den Rest übernimmt PGP Desktop Email.

### Verschlüsselte E-Mail-Nachrichten senden

Nach der Installation wird PGP Desktop Email zur Überwachung des E-Mail-Verkehrs zwischen dem E-Mail-Client und dem Mail-Server eingesetzt.

Eingehende Nachrichten werden von PGP Desktop Email abgefangen, bevor sie den Posteingang erreichen. Es wird automatisch versucht, sie zu entschlüsseln und zu verifizieren. Für die Entschlüsselung werden Ihre privaten Schlüssel und für die Verifizierung die öffentlichen Schlüssel anderer Anwender verwendet. Nach der Verarbeitung der Nachrichten werden sie von PGP Desktop Email an Ihren Posteingang zugestellt.

In den meisten Fällen müssen Sie keine weiteren Schritte ausführen: Die entschlüsselten eingehenden Nachrichten werden wie jede andere Nachricht im Posteingang angezeigt.

Ausgehende Nachrichten werden von PGP Desktop Email auf dem Weg zum Mail-Server abgefangen und automatisch gemäß den konfigurierten Richtlinien verschlüsselt und signiert.

Auch hier ist kein Benutzereingriff erforderlich. Sie erstellen einfach Ihre Nachrichten in Ihrem E-Mail-Client und senden sie – den Rest übernimmt PGP Desktop Email.

Einzelheiten zur transparenten Verarbeitung eingehender und ausgehender Nachrichten in PGP Desktop Email finden Sie in den folgenden Abschnitten.

### Ankommende Nachrichten

PGP Desktop Email entscheidet anhand des Nachrichteninhalts, was mit einer eingehenden E-Mail-Nachricht geschieht:

- **Weder verschlüsselt noch signiert.** Nachrichten, die weder verschlüsselt noch signiert sind, werden von PGP Desktop Email einfach an Ihr E-Mail-Programm übergeben. Die Nachricht kann ohne weitere Verarbeitung durch PGP Messaging gelesen werden.
- **Verschlüsselt, jedoch nicht signiert.** Verschlüsselte Nachrichten versucht PGP Desktop Email zu entschlüsseln, damit Sie sie lesen können. Dazu durchsucht PGP Desktop zunächst Ihren Schlüsselbund nach dem privaten Schlüssel, der die Nachricht entschlüsseln kann. Wenn PGP Desktop Email den privaten Schlüssel gefunden hat, wird die Nachricht damit entschlüsselt und an den E-Mail-Client übergeben. Wenn PGP Desktop Email den privaten Schlüssel nicht finden kann, wird die Nachricht verschlüsselt an den E-Mail-Client übergeben. Die Nachricht sieht ungefähr wie folgt aus.

```
-----BEGIN PGP MESSAGE-----  
Version: PGP Desktop 9.6
```

```
qANQR1DBWUdMvpgQkZ1HwBD/0f5F8QkTY+1NVZwQW4xQ/Epu0D0mLRMZVNVQVn  
rVvHPoSAcn6C3ZFp0996akjR1o0Bga62hklpkjQ13QEGpBTqMP1F64TuxqhkplNH  
ISN+7ZEA7EYTT+3EREOH6yGgJ+sQgm65JRjddYYVTG6hGa9F2wX+ZDLAK65rA  
F4ZnQfNvkowMmJ2X5785Z7LEGE5d5Wm68kKB/FF1vFYz1w360gguIXmnm9F8294p  
FnanWanh1R1f/1a/Muys0wKTLpQpDBxhgZvKkaE85gsCrwqxfMAGDEYfrsCabiNe  
rhwJntXsRYvpstmpNBZuVH01jkrXE4YEAPk48M0D1Y154N3xywuvury790d0x01Jh  
o9yh9v5f071orPLFcw8wMLX4qjagds0vqdwQRnFwbwbgds1j02cmjJyQq+bcy  
3PZknIEgbb7CTKak01Cj+y9uSAF0h491A9QLYHtWMLuHYV/1/wEBPF2P3j6yVACV  
FQRDE08hyZkcc/foQW1Imdo+nymZEQ1tTTDBCAESxmSV+jBwfn0xhuk/Evy1lKaHm  
n27xm9Pdwzxr1q1orxi8Lda7DTJWMA80120C1QZqrqVAmqIKL4CpckYhPuRwIg  
nan80KN/USfZK+v19juxM11550GY20DTL6KnLNGGpT1u6YLSU25B71Ibve330ukJ  
ZMLXqDLAKQFSitPMVekqJPXQrMRL1EYr6H7FcAYMUWxe8w60e7H20wEIme2Y9V  
eVoc55p9Iau7w987Ifbh1odeB+QEWJMAv55JbcaE1ZhxAYLfrIdxBb1REeuQGjmJ  
FUCHF68GgTp9H1Njw92ir5qSintRoh2KmwTa50gBDNnEEAAQ3p8SI+6129FLpGf  
q7/wzmKfngv40gILxyPCrY56p030wAgJehhQDzC9Kekmxd637t/cadEMUSnHC1  
ZTBASchRB+8eN5yRURZ5YqHNVpR/VVN60dPenX4mbrMsc1v4uXRY5v50fGHJTOU  
=8hvs
```

```
-----END PGP MESSAGE-----
```

- **Signiert, jedoch nicht verschlüsselt.** Bei signierten Nachrichten versucht PGP Desktop Email die Signatur zu verifizieren. Der geeignete öffentliche Schlüssel wird in dieser Reihenfolge an den folgenden Orten gesucht: im Standardschlüsselbund, auf dem Keyserver unter „keys.Domain“, wobei „Domain“ die Domain des Absenders der Nachricht ist, dann im PGP Global Directory (unter „keyserver.pgp.com“) und schließlich auf den anderen konfigurierten Keyservern. Wenn PGP Desktop Email den entsprechenden öffentlichen Schlüssel gefunden hat, wird die Signatur verifiziert und an Ihren E-Mail-Client übergeben. Falls der entsprechende öffentliche Schlüssel nicht gefunden wurde, wird die Nachricht unverifiziert an den E-Mail-Client übergeben.
- **Verschlüsselt und signiert.** Bei verschlüsselten und signierten Nachrichten versucht PGP Desktop Email zunächst den privaten Schlüssel für die Entschlüsselung der Nachricht und dann den öffentlichen Schlüssel für ihre Verifizierung zu finden.

### Abgehende Nachrichten

PGP Desktop Email behandelt ausgehende E-Mail-Nachrichten auf der Grundlage von Richtlinien, also Anweisungen, die für beliebige Situationen definiert werden können.

### Standardrichtlinien

PGP Desktop Email umfasst vier Standardrichtlinien:

- **Mailing-Listen-Administratorabfragen.** Administratorabfragen an Mailing-Listen werden als Klartext gesendet, d. h. weder verschlüsselt noch signiert.
- **Mailing-Listen-Sendevorgänge.** Sendevorgänge an Mailing-Listen werden signiert (zur Authentifizierung), jedoch nicht verschlüsselt gesendet.
- **Verschlüsselung erzwingen: [PGP] Vertraulich.** Alle Nachrichten, die in Ihrem E-Mail-Client als „Vertraulich“ markiert sind oder den Text „[PGP]“ in der Betreffzeile enthalten, müssen mit einem gültigen öffentlichen Schlüssel des Empfängers verschlüsselt werden, andernfalls werden sie nicht gesendet. Diese Richtlinie ermöglicht die einfache Verarbeitung von Nachrichten, die verschlüsselt werden **müssen**, damit sie gesendet werden.
- **Opportunistische Verschlüsselung.** Bestimmt, dass alle Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, unverschlüsselt (als Klartext) gesendet werden. Wenn sie sich als letzte Richtlinie in der Liste befindet, ist gewährleistet, dass Ihre Nachrichten, sofern Sie sie nicht als „Vertraulich“ markieren, immer gesendet werden (allerdings als Klartext), selbst wenn kein Schlüssel für die Verschlüsselung gefunden wird.

### Erstellen neuer Richtlinien

PGP Desktop Email bietet die Möglichkeit, zusätzlich zu den vier Standardrichtlinien neue Richtlinien zu erstellen und zu verwenden. Für die Richtlinienerstellung stehen Ihnen vielfältige Kriterien zur Verfügung.

Umfassende Informationen über das Erstellen und Implementieren von Messaging-Richtlinien finden Sie im *PGP Desktop Anwenderhandbuch*.



## Wurde meine Nachricht verschlüsselt?

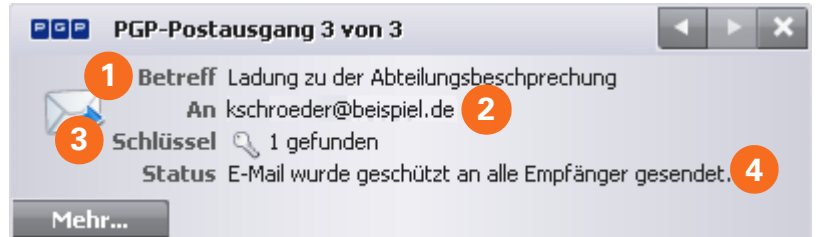
Da PGP Desktop Email automatisch und transparent arbeitet, fragen Sie sich vielleicht gelegentlich, ob Ihre Nachricht tatsächlich verschlüsselt gesendet wurde. Die Antwort lautet wahrscheinlich Ja, es gibt aber Möglichkeiten, die Verschlüsselung zu überprüfen.

### Notifier-Meldungen

PGP Desktop Notifier-Meldungen sind eine Funktion von PGP Desktop Email, die Sie einerseits über die Messaging-Abläufe informiert und Ihnen andererseits deren Steuerung ermöglicht.

Beim Senden einer verschlüsselten Nachricht wird beispielsweise eine Notifier-Meldung mit folgenden Informationen in der rechten unteren Bildschirmcke angezeigt:

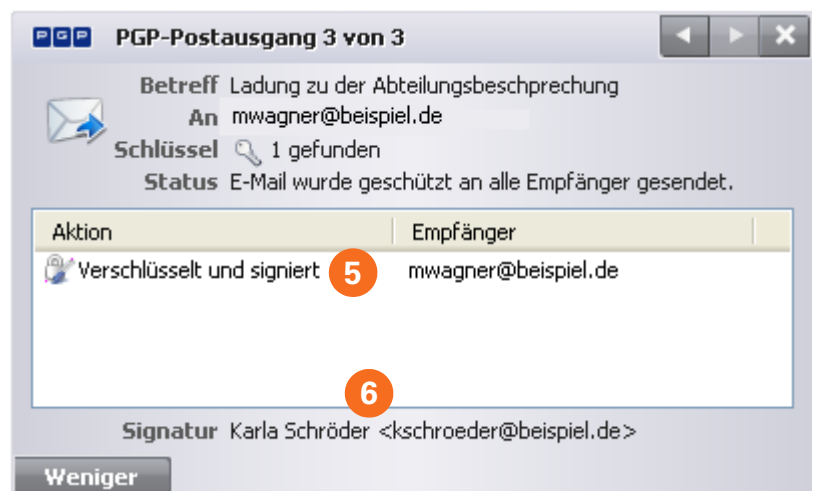
- 1 Betreff
- 2 Empfänger der Nachricht
- 3 Für den Empfänger gefundene Schlüssel
- 4 Status der Nachricht



Wenn Sie weitere Informationen über die gesendete Nachricht wünschen, klicken Sie auf **Mehr**. Nun werden zusätzlich folgende Informationen angezeigt:

- 5 Die Verarbeitungsschritte, die die Nachricht in PGP Desktop Email durchlaufen hat.
- 6 Die Person, von der die Nachricht signiert wurde.

Weitere Information über Notifier-Meldungen finden Sie im *PGP Desktop Anwenderhandbuch*.



### Messaging-Protokoll

Im PGP Desktop Email-Protokoll werden verschiedene Aktionen aufgeführt, die PGP Desktop Email zum Schutz Ihres Nachrichtenverkehrs durchführt.

Für die Nachricht, deren Notifier-Meldungen oben abgebildet sind, wurde im Messaging-Protokoll der folgende Eintrag erzeugt. Er enthält folgende Informationen:

- 7 Den Absender der ausgehenden Nachricht und deren Betreff.
- 8 Die Uhrzeit der Verschlüsselung, die E-Mail-Adresse, für die die Nachricht verschlüsselt wurde, und die E-Mail-Adresse des Absenders.

```
7 Processing outgoing message from Alice Cameron <acameron@example.com>
  with subject: Weekly Status Report
8 08:54:30 Info   Encrypting PGP Partitioned message to mpa@example with key(s):
  08:54:30 Info   'Alice Cameron <acameron@example.com>' (0xF88C695)
```

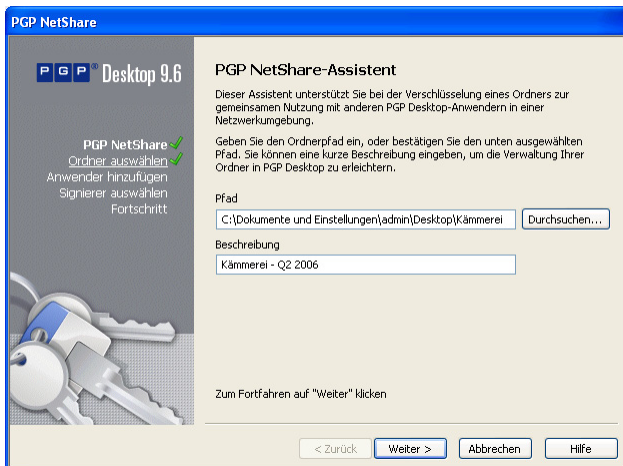
## PGP NetShare verwenden

PGP NetShare ermöglicht berechtigten Anwendern die gemeinsame Nutzung geschützter Dateien. Erstellen Sie zunächst einen geschützten Ordner, und geben Sie dann die Anwender an, die zur Verwendung der Dateien berechtigt sein sollen.

- 1 Klicken Sie im Bedienfeld **PGP NetShare** auf **Ordner hinzufügen**.

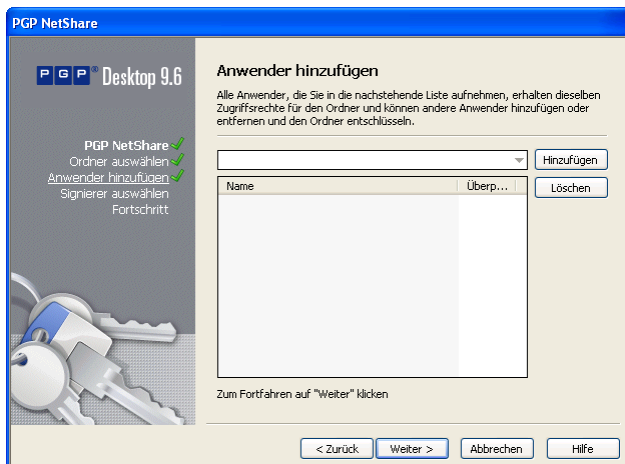


Das Fenster **Ordner auswählen** wird angezeigt.



- 2 Klicken Sie auf **Durchsuchen**, und wählen Sie dann den Ordner aus, den Sie als geschützten Ordner definieren möchten.
- 3 Geben Sie in das Feld **Beschreibung** eine Beschreibung für den geschützten Ordner ein, oder lassen Sie das Feld leer, um den Standardnamen zu übernehmen.
- 4 Klicken Sie auf **Weiter**.

Der Bildschirm **Anwender hinzufügen** wird angezeigt.



- 5 Klicken Sie auf den Pfeil nach unten, wählen Sie einen Anwender aus, und klicken Sie auf **Hinzufügen**, um die berechtigten Anwender für die Dateien im geschützten Ordner anzugeben.

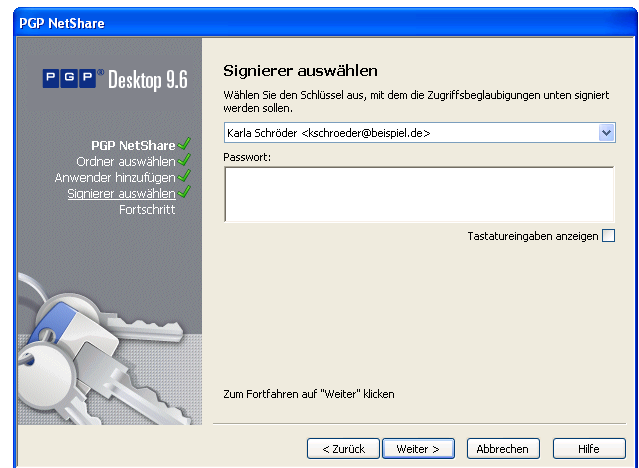
Sie müssen auch sich selbst hinzufügen, wenn Sie ebenfalls zum Zugriff auf die Dateien im geschützten Ordner berechtigt sein möchten.



PGP NetShare informiert die berechtigten Anwender nicht darüber, dass sie auf die geschützten Dateien zugreifen können. Es ist Aufgabe des Erstellers des geschützten Ordners, die berechtigten Anwender darüber zu informieren.

- 9 Klicken Sie auf **Weiter**.

Das Fenster **Signierer auswählen** wird angezeigt.

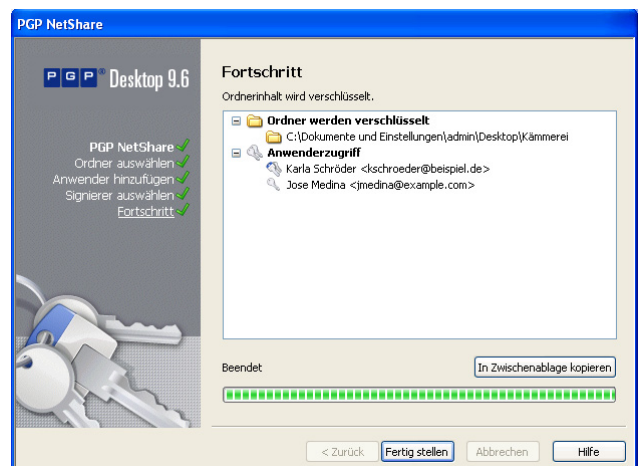


- 10 Wählen Sie einen der privaten Schlüssel am lokalen Schlüsselbund aus, und geben Sie das zugehörige Passwort ein (falls dieses nicht zwischengespeichert ist).

Dieser Schlüssel wird zum Schutz der PGP NetShare-Konfigurationsinformationen für den geschützten Ordner und die darin enthaltenen Dateien verwendet.

- 11 Klicken Sie auf **Weiter**.

Der Bildschirm **Fortschritt** wird angezeigt.



Die Dateien im geschützten Ordner werden verschlüsselt, und die angegebenen Anwender erhalten die Berechtigung zur Verwendung der Dateien.

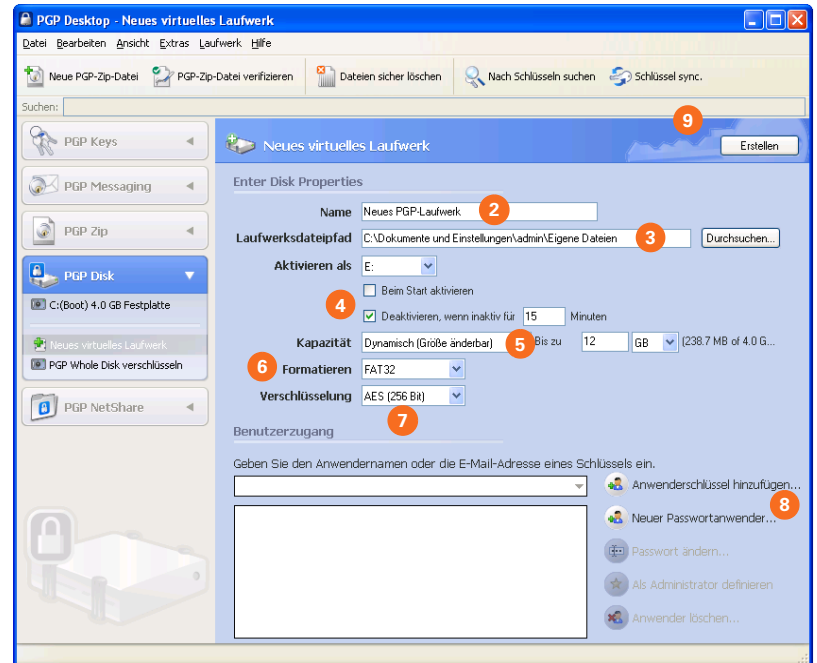
- 12 Klicken Sie auf **Fertig stellen**.



# PGP Virtual Disk-Laufwerke erstellen

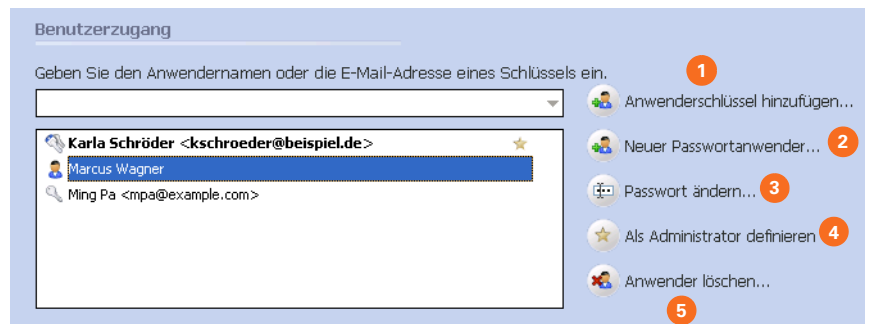
Die Funktion für PGP Virtual Disk-Laufwerke verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit eigenem Laufwerksbuchstaben. Sie können weitere Anwender für ein Laufwerk erstellen und dadurch den autorisierten Personen den Zugriff gestatten.

- 1 Klicken Sie im Bedienfeld **PGP Disk** auf **Neues virtuelles Laufwerk**.
- 2 Geben Sie unter **Name** den Namen des Laufwerks ein.
- 3 Legen Sie unter **Laufwerksdateipfad** den Laufwerkspfad fest.
- 4 Wählen Sie Ihre Aktivierungseinstellungen aus:
  - Wählen Sie unter **Aktivieren als** einen Laufwerksbuchstaben für das Laufwerk aus.
  - Aktivieren Sie **Beim Start aktivieren**, wenn das neue Laufwerk beim Starten automatisch aktiviert werden soll.
  - Aktivieren Sie **Deaktivieren, wenn inaktiv für x Minuten**, damit das Laufwerk automatisch deaktiviert wird, wenn es die angegebene Zahl von Minuten inaktiv war.
- 5 Wählen Sie unter **Kapazität** den Eintrag **Dynamisch (Größe änderbar)**, wenn das Laufwerk beim Hinzufügen von Dateien größer werden soll, oder **Feste Größe**, wenn die Laufwerksgröße unverändert bleiben soll.
- 6 Geben Sie unter **Format** ein Dateisystemformat für das Laufwerk an.
- 7 Legen Sie unter **Verschlüsselung** den Verschlüsselungsalgorithmus für das Laufwerk fest.
- 8 Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die sich mit asymmetrischer Kryptographie authentifizieren, oder klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die sich mit Passwörtern authentifizieren.
- 9 Klicken Sie auf **Erstellen**.



Im Abschnitt **Benutzerzugang** steuern Sie die bestehenden Anwender eines PGP Virtual Disk-Laufwerks:

- 1 Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die sich mit asymmetrischer Kryptographie authentifizieren.
- 2 Klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die sich mit Passwörtern authentifizieren.
- 3 Wenn Sie das Passwort eines Passwortanwenders ändern möchten, wählen Sie ihn aus und klicken auf **Passwort ändern**.
- 4 Markieren Sie einen Anwender, und klicken Sie auf **Als Administrator definieren**, um dem Anwender Administratorrechte zuzuweisen.
- 5 Markieren Sie einen Anwender, und klicken Sie auf **Löschen**, um den Anwender zu löschen.



## PGP WDE - Bewährte Methoden

PGP Corporation empfiehlt für die Vorbereitung der Laufwerkverschlüsselung die nachfolgenden bewährten Methoden. Bitte beachten Sie die nachfolgenden Empfehlungen, um Ihre Daten während und nach der Verschlüsselung zu schützen.

Bevor Sie Ihr Laufwerk verschlüsseln, müssen Sie einige Aufgaben durchführen, um die erfolgreiche Erstverschlüsselung des Laufwerks sicherzustellen.

- 1 Stellen Sie fest, ob Ihr Ziellaufwerk unterstützt wird.** Die PGP WDE-Funktion sperrt Desktop- oder Laptop-Laufwerke (entweder Partitionen, oder das gesamte Laufwerk), externe Laufwerke und USB-Flash-Laufwerke. CD-RW/DVD-RWs und Server werden NICHT unterstützt. Informationen zu den unterstützten Laufwerktypen finden Sie im *PGP Desktop Anwenderhandbuch* in Kapitel 6.
- 2 Sichern Sie das Laufwerk vor der Verschlüsselung.** Erstellen Sie vor dem Verschlüsseln des Laufwerks unbedingt eine Sicherungskopie um zu vermeiden, dass im Falle des Verlusts oder Diebstahls Ihres Laptops oder Computers, oder falls das Laufwerk nicht mehr entschlüsselt werden kann, Daten verloren gehen.
- 3 Vergewissern Sie sich vor der Verschlüsselung vom einwandfreien Zustand des Laufwerks.** Falls PGP WDE während der Verschlüsselung Fehler erkennt, wird die Verschlüsselung angehalten, um Ihnen Gelegenheit zu geben, den Laufwerkfehler zu beheben. Es ist jedoch effizienter, derartige Fehler vor Beginn der Verschlüsselung zu beheben. Weitere Informationen finden Sie unter [Laufwerk vor der Verschlüsselung überprüfen](#).
- 4 Erstellen Sie ein Wiederherstellungslaufwerk.** Wenngleich das Risiko äußerst gering ist, dass ein Master Boot Record auf einem mit PGP Whole Disk Encryption geschützten Startlaufwerk oder einer Partition beschädigt wird, so ist diese Möglichkeit dennoch vorhanden. Erstellen Sie deshalb vor dem Verschlüsseln eines Startlaufwerks oder einer Partition mit PGP Whole Disk Encryption ein Wiederherstellungslaufwerk. Anweisungen zum Erstellen eines Wiederherstellungslaufwerks finden Sie unter [PGP WDE - Bewährte Methoden \(Forts.\)](#).
- 5 Stellen Sie sicher,** dass Ihnen für die Dauer der Verschlüsselung eine Netzstromversorgung zur Verfügung steht. Siehe [Gleichmäßige Stromversorgung während der gesamten Verschlüsselung auf Seite 11](#).
- 6 Führen Sie zur Sicherstellung der Software-Kompatibilität einen Versuchstest aus.** PGP Corporation empfiehlt als bewährte Sicherheitsmaßnahme, PGP WDE vor der Anwendung auf eine umfangreichere Computer-Gruppe zunächst an einer reduzierten Anzahl an Systemen zu testen, um Konflikte mit der darauf befindlichen Software auszuschließen. Dies ist insbesondere in Umgebungen sinnvoll, die ein standardisiertes COE-Image (COE: Corporate Operating Environment) verwenden. Eine Liste mit Software-Produkten, deren Inkompatibilität mit PGP WDE bekannt ist, finden Sie unter [Versuchstest zur Sicherstellung der Software-Kompatibilität ausführen auf Seite 11](#).
- 7 Führen Sie eine Laufwerk-wiederherstellung auf einem entschlüsselten Laufwerk durch.** Falls Wiederherstellungsaktivitäten auf einem mit PGP Whole Disk Encryption (WDE) geschützten Laufwerk erforderlich sein sollten, empfiehlt PGP Corporation als bewährte Maßnahme, das Laufwerk nach Möglichkeit zuerst zu entschlüsseln. Verwenden Sie hierzu entweder die Option **PGP Desktop Disk > Entschlüsseln**, Ihr vorbereitetes PGP WDE-Wiederherstellungslaufwerk, oder verbinden Sie die Festplatte über ein USB-Kabel mit einem zweiten System und führen Sie die Entschlüsselung über das zweite System mithilfe der dort vorhandenen PGP Desktop-Software durch. Wenn das Laufwerk entschlüsselt ist, fahren Sie mit der Wiederherstellung fort.

## Laufwerk vor der Verschlüsselung überprüfen

PGP Corporation wählt bei der Verschlüsselung von Laufwerken bewusst einen konservativen Ansatz, um den Verlust von Daten zu vermeiden. Während der Verschlüsselung einer Festplatte kommt es nicht selten zu CRC-Fehlern (CRC: Cyclic Redundancy Check). Falls PGP WDE auf eine Festplatte oder Partition mit beschädigten Sektoren trifft, wird der Verschlüsselungsprozess standardmäßig angehalten. Sie haben dadurch die Gelegenheit, das Problem vor dem Fortsetzen des Verschlüsselungsprozesses zu beheben und auf diese Weise eine mögliche Beschädigung der Festplatte oder Datenverlust zu vermeiden.

Damit der Verschlüsselungsprozess nicht unterbrochen werden muss, empfiehlt PGP Corporation von Beginn an ein fehlerfreies Laufwerk zu verwenden, bzw. etwaige Laufwerkfehler vor der Verschlüsselung zu beheben.

- Verwenden Sie vor dem Starten von PGP WDE ein Festplattenprüfprogramm eines Drittherstellers, das in der Lage ist, eine grundlegende Integritätsprüfung vorzunehmen und etwaige Konflikte mit dem Laufwerk, die zu CRC-Fehlern führen könnten, zu beheben. Das Festplattenprüfprogramm von Microsoft Windows (chkdsk.exe) ist nicht ausreichend, um derartige Probleme auf der Zielfestplatte zu erkennen. Verwenden Sie stattdessen Software-Produkte wie SpinRite oder Norton Disk Doctor™. Diese Software-Anwendungen sind in der Lage Fehler zu beheben, die anderenfalls zur Unterbrechung des Verschlüsselungsprozesses führen würden.
- Es hat sich bewährt, stark fragmentierte Laufwerke vor ihrer Verschlüsselung zu defragmentieren.

## PGP WDE - Bewährte Methoden (Forts.)

### Wiederherstellungs-CD erstellen

Bei den folgenden Anweisungen wird exemplarisch Software von Roxio verwendet. Die tatsächlich durchzuführenden Schritte sind möglicherweise nicht identisch.

- 1 Stellen Sie sicher, dass auf Ihrem System PGP Desktop für Windows und Roxio Easy Media Creator, oder Roxio Easy CD Creator (oder eine andere Software, die über ein ISO-Image eine CD erstellen kann) installiert sind.
- 2 Öffnen Sie Roxio Easy Media Creator, bzw. Roxio Easy CD Creator und wählen Sie die Option zur Erstellung eines Daten-CD-Projekts aus.
- 3 Wählen Sie im Menü **File** (Datei) die Option **Record CD from CD Image** (CD über CD-Image aufnehmen) aus.
- 4 Wählen Sie im Menü **Files of Type** (Dateityp) die Option **ISO Image Files (ISO)** (ISO-Image-Dateien) aus.
- 5 Navigieren Sie ins PGP-Verzeichnis. Der Standardspeicherort lautet: **C:\Programme\PGP Corporation\PGP Desktop\**
- 6 Wählen Sie **bootg.iso** aus und klicken Sie auf **Open** (Öffnen).

- 7 Legen Sie in eines der CD-Laufwerke Ihres Systems eine leere, aufnahmefähige CD ein.
- 8 Klicken Sie im Bildschirm **Record CD Setup** (CD-Aufzeichnung-Setup) auf **Start Recording** (Aufzeichnung starten).
- 9 Wenn der Brennvorgang der Datei auf der CD abgeschlossen ist, klicken Sie auf **OK**.
- 10 Nehmen Sie die Wiederherstellungs-CD aus dem Laufwerk und versehen Sie sie mit einer geeigneten Beschriftung.



PGP WDE-Wiederherstellungs-Laufwerke sind nur mit der Version von PGP Desktop kompatibel, über die die Wiederherstellungs-CD erstellt wurde. Wenn Sie beispielsweise versuchen, mithilfe einer 9.0.x-Wiederherstellungs-CD ein mit PGP WDE 9.6-Software geschütztes Laufwerk zu entschlüsseln, wird das PGP WDE 9.6-Laufwerk unbrauchbar.

### Gleichmäßige Stromversorgung während der gesamten Verschlüsselung

Da die Verschlüsselung ein CPU-intensiver Prozess ist, kann die Verschlüsselung nicht auf einem akkubetriebenen Laptop-Computer gestartet werden. Der Computer **muss** über das Netz betrieben werden. Falls ein Laptop-Computer während des Erstverschlüsselungsprozesses (oder einem späteren Entschlüsselungs- oder Neuverschlüsselungsprozess) in den Akkumodus wechselt, wird PGP WDE angehalten. Wenn die Netzversorgung wiederhergestellt ist, wird der Verschlüsselungs-, Entschlüsselungs- bzw. Neuverschlüsselungsprozess automatisch fortgesetzt.

Unabhängig von der von Ihnen verwendeten Art von Computer, darf die Stromversorgung Ihres Systems während des Verschlüsselungsprozesses nicht unterbrochen werden, oder das System anderweitig unvermittelt heruntergefahren werden, es sei denn, Sie haben die Option **Stromausfallschutz** ausgewählt.

Trennen Sie nicht das Netzkabel nicht vom System, solange der Verschlüsselungsprozess noch andauert. Falls Die Gefahr besteht, dass die Stromversorgung während der Verschlüsselung unterbrochen wird, oder falls Sie nicht über eine unterbrechungsfreie Stromversorgung für Ihren Computer verfügen, sollten Sie die Option **Stromausfallschutz**, gemäß der Beschreibung im *PGP Desktop Anwenderhandbuch*, verwenden.



Dies gilt auch für entfernbare Laufwerke in Form von USB-Geräten. Falls Sie die Option **Stromausfallschutz** nicht ausgewählt haben, und das Gerät während der Verschlüsselung entfernt wird, besteht die Gefahr, dass das Gerät dadurch beschädigt wird.

### Versuchstest zur Sicherstellung der Software-Kompatibilität ausführen

Einige Software-Programme zur Laufwerksicherung sind nicht kompatibel mit PGP WDE und können zu schwerwiegenden Laufwerkproblemen führen, die u. a. bis hin zum Datenverlust reichen.

Bitte beachten Sie die folgenden bekannten Kompatibilitätsprobleme und überprüfen Sie die Versionshinweise von PGP Desktop in Hinblick auf aktuelle Ergänzungen dieser Liste.

Folgende Software-Produkte sind nicht kompatibel:

- **CompuTrace im MBR-Modus.** PGP Whole Disk Encryption ist ausschließlich mit der BIOS-Konfiguration des Absolute Software CompuTrace-Produkts für Laptop-Sicherheit und Überwachung kompatibel. Die Verwendung von CompuTrace im MBR-Modus ist nicht kompatibel.

- **Utimaco Safeguard Easy 3.x** ist nicht kompatibel mit der Funktion PGP Whole Disk Encryption. Installieren Sie dieses Produkt nicht auf einem System, auf dem PGP Desktop vorhanden ist und installieren Sie PGP Desktop auch nicht auf einem System mit Utimaco Safeguard Easy 3.x.
- **Festplatten-Verschlüsselungsprodukte von GuardianEdge Technologien:** Die Produkte Encryption Anywhere Hard Disk und Encryption Plus Hard Disk, ehemals bekannt unter dem Namen PC Guardian.

Die folgenden Programme können zwar neben PGP Desktop auf demselben System bestehen, blockieren jedoch die Funktion PGP Whole Disk Encryption:

- **Safeboot Solo**
- **SecureStar SCPP**
- **Pointsec.**

# Laufwerk mit PGP WDE verschlüsseln

Die Funktion PGP WDE sperrt den gesamten Inhalt Ihres Systems, eines externen Laufwerks, oder eines von Ihnen angegebenen USB-Flash-Laufwerks.



PGP Corporation empfiehlt Ihnen als bewährte Methode, vor der Verschlüsselung des Laufwerks Ihre Daten zu sichern.

- 1 Klicken Sie im Bedienfeld **PGP Disk** auf **PGP Whole Disk verschlüsseln**.



- 2 Wählen Sie das Laufwerk oder die Partition aus, das oder die verschlüsselt werden soll.
- 3 Aktivieren Sie **Maximale CPU-Auslastung**, um das Laufwerk möglichst schnell zu schützen. Der Verschlüsselungsvorgang hat Vorrang vor den anderen Prozessen im System.
- 4 Aktivieren Sie **Stromausfallschutz**, wenn Sie während des Verschlüsselungsvorgangs einen Stromausfall befürchten.

Wenn **Stromausfallschutz** aktiviert ist, kann der Verschlüsselungsvorgang nach einer Unterbrechung problemlos fortgesetzt werden. Allerdings kann die Verschlüsselung mit dieser Option länger dauern.

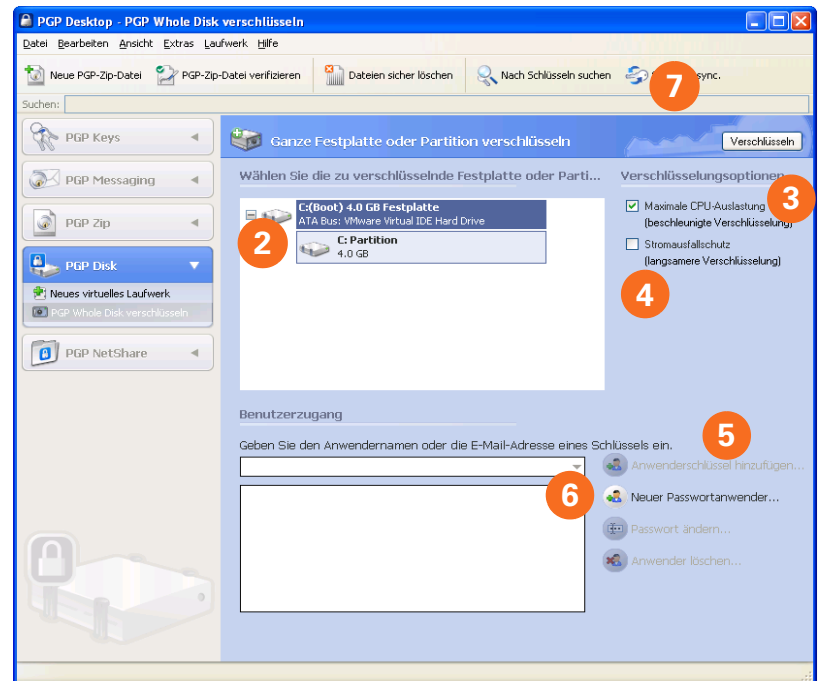
- 5 Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die sich mit asymmetrischer Kryptographie bei dem mit Whole Disk Encryption verschlüsselten Laufwerk authentifizieren können.

Wenn Sie eine Festplatte verschlüsseln, kann nur ein PGP-Schlüsselpaar auf einem USB-Token Aladdin eToken verwendet werden. Wenn Sie eine Partition oder einen Wechseldatenträger (keine Festplatte) verschlüsseln, kann ein beliebiges Schlüsselpaar auf dem System verwendet werden.

- 6 Klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die sich mit Passwörtern authentifizieren.

Bei der Verschlüsselung des Boot-Laufwerks haben Sie die Möglichkeit, Ihr eigenes Windows-Anmeldepasswort zu verwenden, so dass Sie Ihre Zugriffsbeglaubigungen nur einmal beim Systemstart eingeben müssen.

- 7 Klicken Sie auf **Verschlüsseln**.



Verwenden Sie für die Verschlüsselung von Daten auf Disketten oder CD-RWs PGP Virtual Disk-Laufwerke, nicht PGP WDE. PGP WDE ist mit Dual-Boot-Systemen nicht kompatibel.

Sicherungssoftware funktioniert mit PGP WDE ohne Einschränkungen. Alle von der Software gesicherten Dateien werden vor dem Anlegen der Sicherungskopie entschlüsselt.

## PGP Zip-Archive erstellen

PGP Zip-Archive ermöglichen es Ihnen, beliebige Kombinationen von Dateien und Ordnern in ein komprimiertes und portables Archiv einzufügen. Es gibt vier Arten von PGP Zip-Archiven:

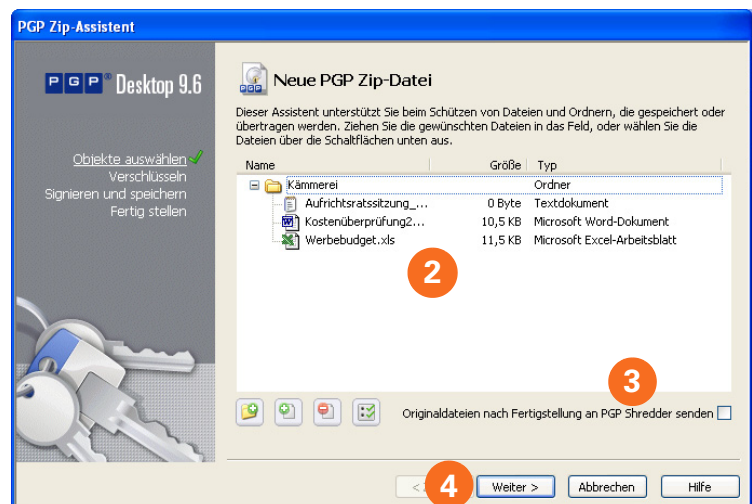
- **Empfängerschlüssel.** Verschlüsselt das Archiv zu einem öffentlichen Schlüssel. Nur der Besitzer des entsprechenden privaten Schlüssels kann das Archiv öffnen. Dies ist der sicherste PGP Zip-Archivtyp. Die Empfänger müssen PGP Messaging oder PGP Desktop für Windows verwenden.
- **Passwort.** Verschlüsselt das Archiv mit einem Passwort, das den Empfängern mitgeteilt werden muss. Die Empfänger müssen PGP Messaging oder PGP Desktop für Windows verwenden.
- **Selbstentschlüsselndes PGP-Archiv.** Verschlüsselt das Archiv mit einem Passwort, die Empfänger benötigen aber *nicht* PGP Messaging oder PGP Desktop für Windows, um es zu öffnen. Das Passwort muss den Empfängern mitgeteilt werden.
- **Nur signieren.** Signiert das Archiv, ohne es zu verschlüsseln. So können Sie Ihre Identität als Absender bestätigen. Die Empfänger müssen PGP Messaging oder PGP Desktop für Windows verwenden, um das Archiv zu öffnen und zu verifizieren.

Die PGP Zip-Typen „Passwort“ und „Nur signieren“ werden im *PGP Desktop Anwenderhandbuch* ausführlicher beschrieben, als es in diesem Handbuch möglich ist.

- 1 Klicken Sie im Bedienfeld **PGP Zip** auf **Neue PGP-Zip-Datei**.



- 2 Ziehen Sie die Dateien und Ordner, die Sie dem Archiv hinzufügen möchten, in das Feld, oder wählen Sie sie über die Schaltflächen aus.
- 3 Wählen Sie **Originaldateien nach Fertigstellung an PGP Shredder senden**, wenn die hinzugefügten Dateien und Ordner nach dem Erstellen des Archivs sicher gelöscht werden sollen.
- 4 Klicken Sie auf **Weiter**.



- 5 Wählen Sie den gewünschten PGP Zip-Archivtyp:
  - **Empfängerschlüssel**
  - **Passwort**
  - **Selbstentschlüsselndes PGP-Archiv**
  - **Nur signieren**

- 6 Klicken Sie auf **Weiter**.

**Passwort** und **Nur signieren** werden im *PGP Desktop Anwenderhandbuch* ausführlich beschrieben.

Lesen Sie auf den folgenden Seiten den relevanten Abschnitt für den angegebenen PGP Zip-Archivtyp.





## PGP Zip-Archive erstellen (Forts.)

### Empfängerschlüssel

Der Bildschirm **Anwenderschlüssel hinzufügen** wird angezeigt.

- 1 Klicken Sie auf **Hinzufügen**, und wählen Sie auf dem Bildschirm **Anwenderauswahl** die öffentlichen Schlüssel der Personen aus, die das Archiv öffnen können sollen.  
Wenn Sie das Archiv auch selbst öffnen können möchten, müssen Sie auch Ihren eigenen öffentlichen Schlüssel hinzufügen.

- 2 Klicken Sie auf **Weiter**.

- 3 Wählen Sie einen privaten Schlüssel auf dem lokalen System, um das Archiv zu signieren.

- 4 Legen Sie einen Namen und einen Speicherort für das Archiv fest.

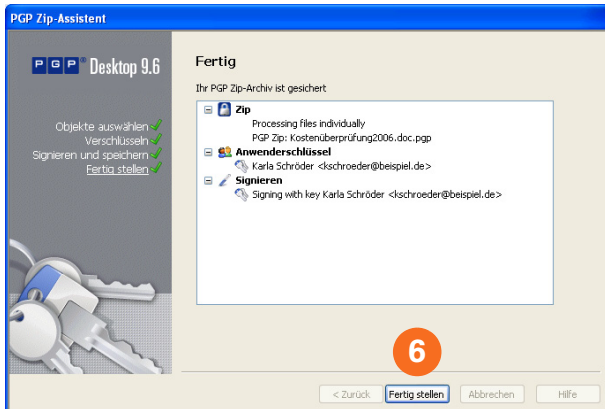
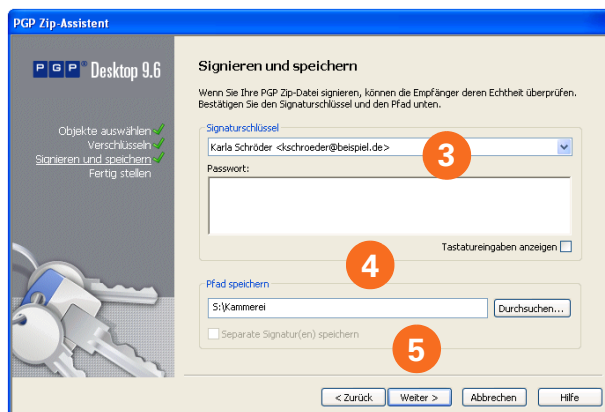
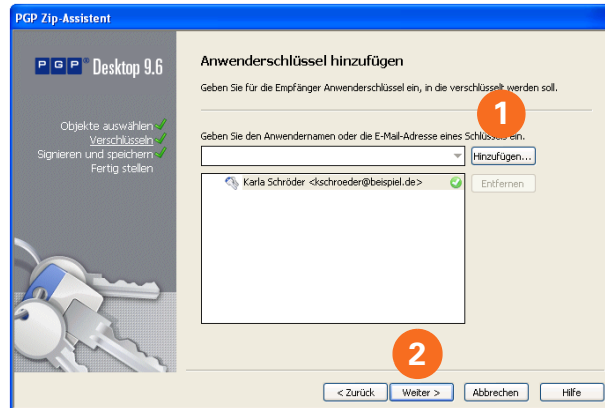
Der Standardname ist der Name der ersten Datei bzw. des ersten Ordners im Archiv. Der Standardspeicherort ist der Speicherort der Dateien und Ordner, die in dem Archiv gespeichert werden.

- 5 Klicken Sie auf **Weiter**.

Das PGP Zip-Archiv wird erstellt.

Auf dem Bildschirm **Fertig** werden Informationen über das neue Archiv angezeigt.

- 6 Klicken Sie auf **Fertig stellen**.



Der PGP Zip-Archivtyp **Passwort** unterscheidet sich nur dadurch vom Typ mit Empfängerschlüsseln, dass anstelle eines Schlüssels ein Passwort zum Schutz des Archivs verwendet wird.



Der PGP Zip-Archivtyp **Nur signieren** unterscheidet sich nur dadurch vom Typ mit Empfängerschlüsseln, dass das Archiv lediglich signiert, nicht aber verschlüsselt wird und daher keine öffentlichen Schlüssel ausgewählt werden.



# PGP Zip-Archive erstellen (Forts.)

## Selbstentschlüsselndes PGP-Archiv

Der Bildschirm **Passwort definieren** wird geöffnet.

- 1 Geben Sie ein Passwort für das selbstentschlüsselnde PGP- Archiv (SDA) ein, und bestätigen Sie es, indem Sie es erneut eingeben.

- 2 Klicken Sie auf **Weiter**.

- 3 Wählen Sie einen privaten Schlüssel auf dem lokalen System, um das Archiv zu signieren.

- 4 Legen Sie einen Namen und einen Speicherort für das Archiv fest.

Der Standardname ist der Name der ersten Datei bzw. des ersten Ordners im Archiv. Der Standardspeicherort ist der Speicherort der Dateien und Ordner, die in dem Archiv gespeichert werden.

- 5 Klicken Sie auf **Weiter**.

Das selbstentschlüsselnde PGP-Archiv wird erstellt.

- 6 Klicken Sie auf **Fertig stellen**.

## Dateien sicher löschen

PGP Shred zerstört Dateien und Ordner vollständig, so dass sie selbst mit der besten Datenwiederherstellungssoftware nicht wiederhergestellt werden können. Auf dem Desktop wird sowohl für PGP Shred als auch für den Windows-Papierkorb ein Symbol angezeigt. Aber nur PGP Shred überschreibt die angegebenen Dateien sofort, so dass sie nicht wiederhergestellt werden können.

Sie können Dateien auf folgende Arten sicher löschen:

- Mit dem PGP Shred-Symbol
- Mit der PGP-Symbolleiste
- Mit dem PGP-Kontextmenü

### Mit dem PGP Shred-Symbol

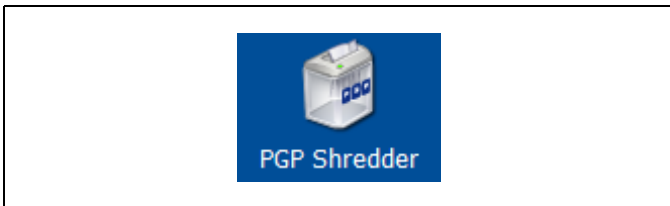
So löschen Sie Dateien sicher mit dem PGP Shred-Symbol:

- 1 Ziehen Sie auf dem Windows-Desktop die Dateien und Ordner, die Sie sicher löschen möchten, auf das PGP Shred-Symbol.

Ein Dialogfeld erscheint, in dem Sie aufgefordert werden, zu bestätigen, dass die Dateien sicher gelöscht werden sollen.

- 2 Klicken Sie auf **Ja**.

Die angegebenen Dateien und Ordner werden sicher gelöscht.



### Mit der PGP-Symbolleiste

So löschen Sie Dateien sicher mit der PGP-Symbolleiste:

- 1 Öffnen Sie PGP Desktop.
- 2 Klicken Sie auf der PGP-Symbolleiste auf **Dateien sicher löschen**.

- 3 Geben Sie an, welche Dateien sicher gelöscht werden sollen.

Klicken Sie bei gedrückter Strg-Taste auf die Dateien, um mehrere Dateien auszuwählen, oder drücken Sie Strg-A, um alle angezeigten Dateien auszuwählen.

- 4 Klicken Sie auf **Öffnen**.

Ein Dialogfeld erscheint, in dem Sie aufgefordert werden, zu bestätigen, dass die Dateien sicher gelöscht werden sollen.

- 5 Klicken Sie auf **Ja**.

Die angegebenen Dateien und Ordner werden sicher gelöscht.



### Mit dem PGP-Kontextmenü

So löschen Sie Dateien sicher in Windows Explorer:

- 1 Öffnen Sie Windows Explorer.
- 2 Klicken Sie mit der rechten Maustaste auf die Dateien oder Ordner, die Sie sicher löschen möchten, und wählen Sie dann **PGP Desktop > Sicheres Löschen von <Dateiname>**.

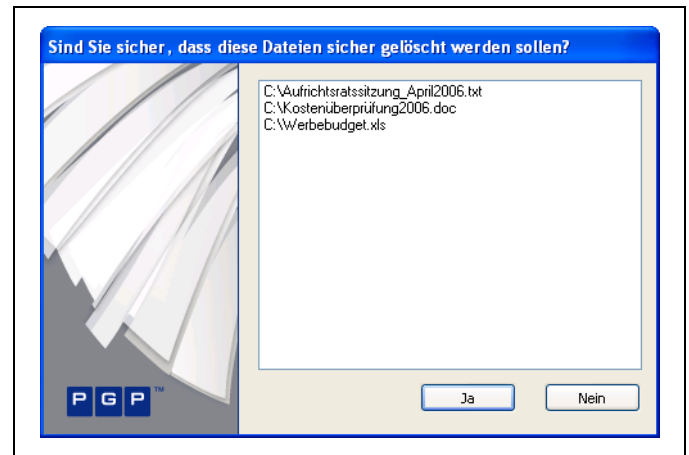
Klicken Sie bei gedrückter Strg-Taste auf die Dateien, um mehrere Dateien auszuwählen, oder drücken Sie Strg-A, um alle angezeigten Dateien auszuwählen.

Wenn Sie mehrere Dateien ausgewählt haben, lautet der Text: **PGP Shred x Objekte**, wobei **x** die Anzahl der markierten Dateien angibt.

Ein Dialogfeld erscheint, in dem Sie aufgefordert werden, zu bestätigen, dass die Dateien sicher gelöscht werden sollen.

- 3 Klicken Sie auf **Ja**.

Die angegebenen Dateien und Ordner werden sicher gelöscht.



Wenn Sie die PGP Shred-Funktion nicht häufig verwenden, können Sie das PGP Shred-Symbol über die PGP-Optionen vom Desktop entfernen: Öffnen Sie das Feld **Optionen**, klicken Sie auf die Registerkarte **Laufwerk**, deaktivieren Sie die Option **Symbol von PGP Shredder auf dem Desktop erstellen**, und klicken Sie auf **OK**.



Sie können mit den PGP-Optionen auch die Anzahl der Durchgänge beim sicheren Löschen steuern (je mehr Durchgänge, umso sicher, aber umso länger dauert der Vorgang auch) oder festlegen, ob Dateien im Windows-Papierkorb beim Leeren sicher gelöscht werden sollen und ob beim sicheren Löschen eine Warnung angezeigt werden soll.

## Freien Speicherplatz sicher löschen

Mit der Funktion zum sicheren Löschen von freiem Speicherplatz wird freier Speicherplatz auf Ihren Laufwerken absolut sicher gelöscht, so dass gelöschte Daten keinesfalls wiederhergestellt werden können. Dabei ist zu berücksichtigen, dass die Bezeichnung „freier Speicherplatz“ irreführend ist. Mit der Funktion zum sicheren Löschen von freiem Speicherplatz werden Teile der Festplatte, die von Windows als leer erkannt wurden, überschrieben. Tatsächlich kann der Speicherplatz leer sein oder aber Dateien enthalten, die laut Windows bereits gelöscht wurden.

Wenn Sie Dateien in den Windows-Papierkorb verschieben und diesen anschließend leeren, werden die Dateien nicht wirklich gelöscht. Windows verhält sich lediglich so, als wäre der Speicherplatz leer, und überschreibt letztendlich die Dateien. Bis zu dem Zeitpunkt, an dem die Dateien überschrieben werden, können sie von einem Angreifer ohne großen Aufwand wiederhergestellt werden. Die Funktion zum sicheren Löschen von freiem Speicherplatz überschreibt diesen „freien Speicherplatz“ so gründlich, dass die Dateien selbst mit der besten Datenwiederherstellungssoftware nicht wiederhergestellt werden können.

So löschen Sie freien Speicherplatz auf Ihren Festplatten sicher:

- 1 Klicken Sie im Menü **Extras** auf **Sicheres Löschen von freiem Speicherplatz**.
- 2 Lesen Sie die einführenden Informationen auf dem Bildschirm **Einführung**, und klicken Sie auf **Weiter**.
- 3 Wählen Sie im Fenster **Informationen sammeln** im Feld **Laufwerk sicher löschen** die Festplatte oder das Laufwerk aus, die bzw. das sicher gelöscht werden soll, und geben Sie die Anzahl der Durchgänge an, die die Funktion zum sicheren Löschen von freiem Speicherplatz durchführen soll.

Für Durchgänge werden die folgenden Richtlinien empfohlen:

- 3 Durchgänge für persönliche Verwendung
- 10 Durchgänge für kommerzielle Verwendung
- 18 Durchgänge für militärische Verwendung
- 49 Durchgänge für optimale Sicherheit

- 4 Aktivieren Sie ggf. die Option **Interne NTFS-Datenstrukturen sicher löschen** (nicht auf allen Systemen verfügbar), und klicken Sie dann auf **Weiter**.

Diese Option löscht auch kleine Dateien (unter 1 KB) in internen Datenstrukturen sicher, die andernfalls nicht sicher gelöscht werden würden.

- 5 Klicken Sie auf dem Bildschirm **Sicheres Löschen durchführen** auf **Sicheres Löschen beginnen**.



Klicken Sie auf **Planen**, um das sichere Löschen des freien Speicherplatzes für einen späteren Zeitpunkt zu planen, statt es sofort durchzuführen. Der Windows-Taskplaner muss auf Ihrem System installiert sein.

Die Dauer des sicheren Löschvorgangs ist von der Anzahl der angegebenen Durchgänge, der Geschwindigkeit der CPU, der Anzahl der ausgeführten anderen Anwendungen usw. abhängig.

- 6 Klicken Sie nach Abschluss des sicheren Löschvorgangs auf **Weiter**.
- 7 Klicken Sie auf dem Bildschirm **Abschließen** auf **Beenden**.

### Hilfe und Unterstützung

#### Verfügbare Produktdokumentation

Diese Dokumente wurden bei der Produktinstallation auf Ihrem System installiert:

- *PGP Desktop für Windows Anwenderhandbuch*
- *PGP Desktop für Windows Versionshinweise*

Über das Hilfemenü im Produkt können Sie kontextbezogene Informationen aufrufen.

#### Kontaktaufnahme mit dem Technischen Support

- Informationen zum Produkt-Support und Kundenservice der PGP Corporation finden Sie im PGP Support-Portal: **<https://www.pgp.com/support>**.
- Die PGP Support-Foren sind unter folgender Adresse verfügbar: **[forums.pgpsupport.com](https://forums.pgpsupport.com)**.
- Weitere Ansprechpartner der PGP Corporation finden Sie im Abschnitt mit Kontakten auf der PGP-Website: **[www.pgp.com/company/contact.html](https://www.pgp.com/company/contact.html)**.