



Was ist PGP Whole Disk Encryption (WDE)?

Das PGP Whole Disk Encryption (WDE)-Produkt ist ein Software-Tool, das mehrere Möglichkeiten zum Schutz Ihrer Daten auf Desktops, Laptops und Wechsellaufwerken bietet.

Mit PGP WDE können Sie folgende Aufgaben ausführen:

- Den gesamten Inhalt Ihres Systems oder eines von Ihnen angegebenen externen oder USB-Flash-Laufwerks sperren.
- 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 auf Windows-Systemen geöffnet werden kann, auf denen PGP Desktop nicht installiert ist.
- 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.

Inhalt

- *Was ist PGP Whole Disk Encryption (WDE)?* (Seite 1)
- *Neu bei PGP Whole Disk Encryption?* (Seite 1)
- *Die Grundlagen* (Seite 1)
- *Was wird installiert?* (Seite 2)
- *Systemvoraussetzungen* (Seite 3)
- *PGP Whole Disk Encryption installieren* (Seite 3)
- *PGP Whole Disk Encryption starten* (Seite 3)
- *Der Hauptbildschirm von PGP Whole Disk Encryption* (Seite 4)
- *PGP WDE zur Verschlüsselung eines Laufwerks verwenden* (Seite 4)
- *PGP Virtual Disk-Laufwerke erstellen* (Seite 7)
- *Ein PGP Zip-Archiv erstellen* (Seite 8)
- *Dateien sicher löschen* (Seite 10)
- *Freien Speicherplatz sicher löschen* (Seite 11)
- *Hilfe und Support* (Seite 12)

Neu bei PGP Whole Disk Encryption?

Diese schrittweise Anleitung erleichtert Ihnen den Einstieg. Sie werden feststellen, dass der Schutz Ihrer Daten mit PGP Whole Disk Encryption (WDE) so einfach ist wie das Drehen eines Schlüssels in einem Schloss.

- Dieser *Schnelleinstieg* enthält Informationen zur

Installation von PGP Whole Disk Encryption und erste Schritte.

- Das *PGP Whole Disk Encryption Anwenderhandbuch* stellt nähere Informationen zu PGP Whole Disk Encryption (WDE) bereit. Dort erfahren Sie, was ein Schlüsselpaar ist, wann und wie Sie ein Schlüsselpaar erstellen können und wie Sie Schlüssel mit anderen Personen austauschen können, um Ihre eigenen Daten zu verschlüsseln und Daten sicher mit anderen auszutauschen.

Hinweis: Eine Lizenz für PGP Whole Disk Encryption bietet Ihnen Zugriff auf einen bestimmten Satz von PGP WDE-Funktionen. Manche anderen Funktionen von PGP Whole Disk Encryption erfordern möglicherweise eine andere Lizenz. Nähere Informationen finden Sie im Abschnitt über Lizenzen im *PGP Whole Disk Encryption Anwenderhandbuch*.

- Informationen zur Implementierung, Verwaltung und Richtliniendurchsetzung für PGP Whole Disk Encryption finden Sie im *Administrator-Handbuch für PGP Universal Server*.

Die Grundlagen

PGP Whole Disk Encryption verwendet Schlüssel zur Verschlüsselung, Signatur, Entschlüsselung und Verifikation Ihrer Nachrichten.

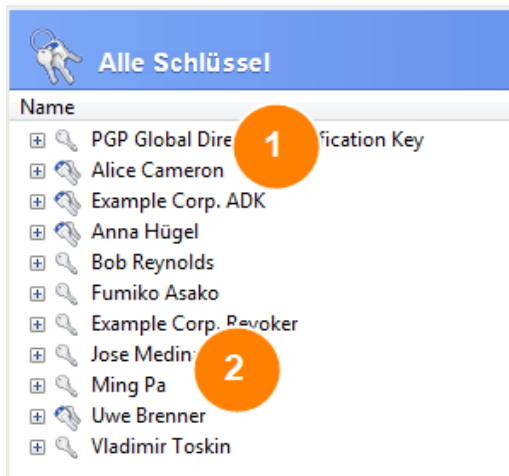
Nach der Installation werden Sie von PGP Whole Disk Encryption aufgefordert, ein PGP Schlüsselpaar zu erstellen. Ein Schlüsselpaar ist die Kombination eines privaten Schlüssels und eines öffentlichen Schlüssels.

- Wie der Name schon nahelegt, behalten Sie Ihren *privaten Schlüssel* und das zugehörige Passwort für sich. Wenn eine andere Person Ihren privaten Schlüssel und das Passwort erfährt, kann sie Ihre Nachrichten lesen und sich anderen gegenüber für Sie ausgeben. Ihr privater Schlüssel entschlüsselt eingehende verschlüsselte Nachrichten und signiert ausgehende Nachrichten.
- Ihren *öffentlichen Schlüssel* können Sie ruhig ausgeben. Er hat kein Passwort. Ihr öffentlicher Schlüssel verschlüsselt Nachrichten, die nur Ihr privater Schlüssel entschlüsseln kann und er verifiziert Ihre signierten Nachrichten.

Ihr Schlüsselbund umfasst Ihre Schlüsselpaare und die öffentlichen Schlüssel von anderen, die Sie zur Versendung von verschlüsselten Nachrichten an diese Personen verwenden. Klicken Sie auf das PGP Bedienfeld „Schlüssel“, um die Schlüssel an Ihrem Schlüsselbund anzuzeigen:

1. Das Symbol für ein PGP-Schlüsselpaar hat zwei Schlüssel, die den privaten und den öffentlichen Schlüssel anzeigen. Alice Cameron, zum Beispiel, hat in dieser Illustration ein PGP-Schlüsselpaar.

- Die Symbole für die öffentlichen Schlüssel von anderen haben nur einen Schlüssel. Der öffentliche Schlüssel von Ming Pa, zum Beispiel, wurde dem in dieser Illustration abgebildeten Schlüsselbund hinzugefügt.



Was wird installiert?

PGP Whole Disk Encryption verwendet Lizenzen zur Bereitstellung von Zugang zu den von Ihnen erworbenen Funktionen. Je nach Lizenz können einige oder alle Anwendungen der PGP Whole Disk Encryption-Produktfamilie genutzt werden.

Dieses Dokument enthält eine Anleitung zur Anzeige der durch Ihre Lizenz aktivierten Funktionen.



PGP Whole Disk Encryption (WDE)

ist eine Anwendung der PGP Desktop-Produktfamilie. Mit PGP Whole Disk Encryption (WDE) kann der gesamte Inhalt Ihres Systems oder eines von Ihnen angegebenen externen oder USB-Flash-Laufwerks gesperrt werden. Boot-Sektoren, Systemdateien und Auslagerungsdateien werden alle verschlüsselt. Bei kompletter Laufwerkverschlüsselung des Boot-Laufwerks brauchen Sie sich bei Verlust oder Diebstahl Ihres Computers keine Sorgen zu machen: zum Zugriff auf Ihre Daten würde ein Angreifer das entsprechende Passwort benötigen.

Weitere Komponenten von PGP Whole Disk Encryption beinhalten:



PGP Virtual Disk-Laufwerke —

Verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit seinem eigenen Laufwerksbuchstaben. Eine PGP Virtual Disk ist der perfekte Speicherort für Ihre vertraulichen Dateien; sie sind dort so sicher gespeichert wie in einem Safe. Wenn die Safetür geöffnet ist (d.h. wenn das Laufwerk aktiviert ist), können Sie dort gespeicherte Dateien ändern, Dateien herausnehmen und Dateien hineinstellen. Anderenfalls (wenn das Laufwerk deaktiviert ist) sind alle Daten auf dem Laufwerk geschützt.



PGP Zip — Fügt einem verschlüsselten, komprimierten, portablen Archiv jede beliebige Kombination von Dateien und Ordnern hinzu. PGP Desktop muss auf dem System installiert sein, damit ein PGP Zip-Archiv erstellt oder geöffnet werden kann. PGP Zip ist ein Werkzeug zur sicheren Archivierung Ihrer sensiblen Daten zum Zwecke der Verteilung an andere oder Datensicherung.

Selbstentschlüsselnde PGP-Archive (SDAs)

— Platziert Dateien und Ordner in ein verschlüsseltes, komprimiertes Paket, das auf Windows-Systemen, auf denen keine PGP-Software installiert ist, geöffnet werden kann. SDAs sind die perfekte Lösung zum sicheren Austausch von Dateien mit einer Person, die die PGP Software nicht installiert hat.



PGP Shredder — Zur vollständigen Vernichtung von Dateien und Ordnern, so dass sie selbst mit Dateiwiederherstellungssoftware nicht wiederhergestellt werden können. Wenn eine Datei über den Windows-Papierkorb entfernt wird, wird sie nicht wirklich gelöscht; sie verbleibt auf Ihrem Laufwerk, bis sie schließlich überschrieben wird. Bis zu dem Zeitpunkt kann diese Datei leicht von einem Angreifer wiederhergestellt werden. PGP Shredder hingegen überschreibt Dateien sofort mehrfach. Das ist so effektiv, dass diese Dateien selbst mit hochentwickelter Laufwerkswiederherstellungssoftware nicht wiederhergestellt werden können. Diese Funktion löscht auch freien Speicherplatz auf Ihren Laufwerken sicher, so dass Ihre gelöschten Daten wirklich nicht wiederherstellbar sind.



Schlüsselverwaltung — PGP Whole Disk Encryption verwaltet auch PGP-Schlüssel, d. h. sowohl Ihre Schlüsselpaare als auch die öffentlichen Schlüssel von anderen. Sie verwenden Ihren privaten Schlüssel zur Entschlüsselung von Nachrichten, die Ihnen auf Ihren öffentlichen Schlüssel verschlüsselt zugeschickt werden, sowie zur Sicherung Ihrer PGP Virtual Disk-Laufwerke. Öffentliche Schlüssel werden zur Verschlüsselung von Nachrichten für andere Personen oder zum Hinzufügen von Anwendern zu PGP Virtual Disk-Laufwerken verwendet.

Systemvoraussetzungen

- Microsoft Windows 2000 (Servicepack 4), Windows Server 2003 (Servicepack 1), Windows XP (Servicepack 1, 2, 3 oder 3; 32-Bit und 64-Bit-Versionen), Windows Vista (alle 32-Bit- und 64-Bit-Versionen, einschl. Servicepack 1), Microsoft Windows XP Tablet PC Edition 2005 (angeschlossene Tastatur notwendig)

Hinweis: Die oben aufgeführten Betriebssysteme werden nur dann unterstützt, wenn die neuesten Hotfixes und Sicherheitspatches von Microsoft installiert wurden.

PGP Whole Disk Encryption (WDE) erfordert Windows 2000 (Servicepack 4), Windows XP (Servicepack 1 oder 2) oder Windows Vista; unter Windows 2000 Server oder 2003 Server wird es *nicht* unterstützt.

- 512 MB RAM
- 64 MB Festplattenspeicher

PGP Whole Disk Encryption installieren

PGP Corporation empfiehlt, alle geöffneten Anwendungen zu schließen, bevor die Installation gestartet wird. Der Installationsprozess erfordert einen Systemneustart.

Hinweis: Wenn Sie PGP Whole Disk Encryption in einer mit PGP Universal Server verwalteten Umgebung verwenden, ist Ihre PGP Whole Disk Encryption-Installationssoftware möglicherweise mit spezifischen Funktionen und/oder Einstellungen konfiguriert.

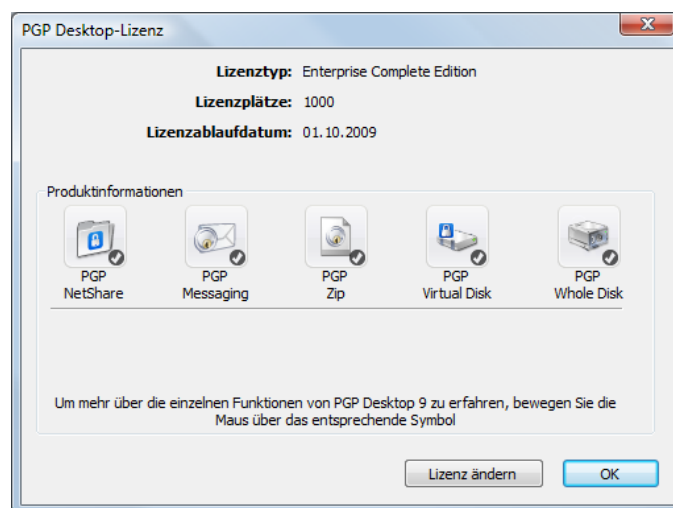
➤ So installieren Sie PGP Whole Disk Encryption

1. Suchen Sie das heruntergeladene PGP Whole Disk Encryption-Installationsprogramm.
Das Installationsprogramm wurde möglicherweise von Ihrem PGP-Administrator mit dem Bereitstellungstool Microsoft SMS verteilt.
2. Doppelklicken Sie auf das Installationsprogramm.

3. Folgen Sie der Anleitung auf dem Bildschirm.
4. Starten Sie das System auf die entsprechende Anweisung hin neu.
5. Befolgen Sie beim Neustart die Anweisungen auf dem Bildschirm zur Konfiguration von PGP Whole Disk Encryption.

Lizenzierung

Um zu sehen, welche Funktionen von Ihrer PGP-Lizenz unterstützt werden, öffnen Sie PGP Whole Disk Encryption und wählen Sie **Hilfe > Lizenz**. Die Funktionen mit einer Kontrollmarkierung werden von der aktiven Lizenz unterstützt.



PGP Whole Disk Encryption starten

Sie können PGP Whole Disk Encryption auf folgende Arten starten:

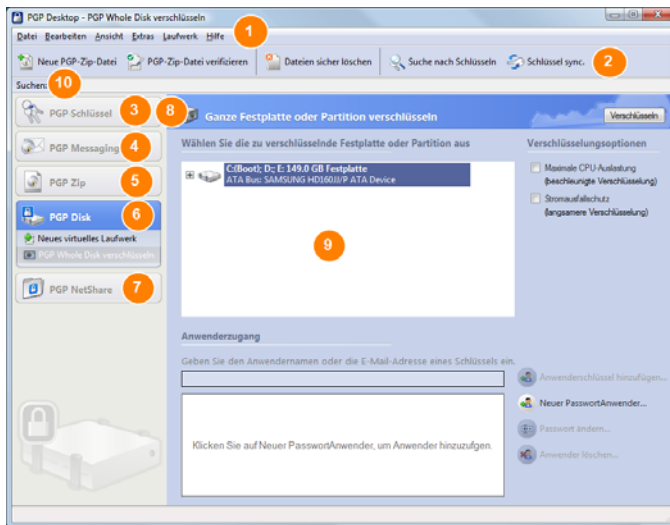
- Doppelklicken Sie auf das PGP Tray-Symbol.



- Rechtsklicken Sie auf das PGP Tray-Symbol und wählen Sie dann **PGP Whole Disk Encryption öffnen**.
- Wählen Sie im Startmenü **Programme > PGP > PGP Whole Disk Encryption**.

Der Hauptbildschirm von PGP Whole Disk Encryption

Das Anwendungsfenster von PGP Whole Disk Encryption ist die primäre Benutzeroberfläche des Produkts.



Der Hauptbildschirm von PGP Whole Disk Encryption umfasst:

- 1 Menüleiste.** Gibt Zugang zu den Befehlen von PGP Whole Disk Encryption. Die Zusammenstellung der Menüs auf der Menüleiste ändert sich in Abhängigkeit davon, welches Bedienfeld ausgewählt wird.
- 2 Symbolleiste.** Auf diesem Steuerelement sind die am häufigsten benötigten Funktionen angeordnet. Sie können ein neues PGP Zip-Archiv erstellen, ein bestehendes PGP Zip-Archiv verifizieren, ausgewählte Dateien sicher löschen, nach einem Schlüssel suchen, Ihre Schlüssel synchronisieren und in den Anwender-IDs der Schlüssel, die gegenwärtig im Arbeitsbereich "PGP Keys" angezeigt werden, nach Text suchen.
- 3 Bedienfeld „PGP Keys“.** Mit diesem Symbol verwalten Sie die PGP-Schlüssel.
- 4 Bedienfeld „PGP Messaging“.** Mit diesem Symbol steuern Sie PGP Messaging.
- 5 Bedienfeld „PGP Zip“.** Mit diesem Bedienfeld steuern Sie die Funktionen von PGP Zip sowie des PGP Zip-Assistenten, der Sie bei der Erstellung neuer PGP Zip-Archive unterstützt.
- 6 Bedienfeld „PGP Disk“.** Mit diesem Symbol steuern Sie PGP Disk.
- 7 Bedienfeld „PGP NetShare“.** Mit diesem Symbol steuern Sie PGP NetShare.

- 8 Bedienfeldsteuerung ein-/ausblenden.** Mit diesem Symbol blenden Sie die Bedienfelder ein oder aus.

- 9 Arbeitsbereich von PGP Whole Disk Encryption.** Hier werden neben verschiedenen Informationen die Aktionen angezeigt, die Sie für das ausgewählte Bedienfeld durchführen können.

- 10 Suchfeld "PGP Keys".** Hier können Sie nach Schlüsseln in Ihrem Schlüsselbund suchen. Wenn Sie in diesem Feld Text eingeben, zeigt PGP Whole Disk Encryption Suchergebnisse von Namen und E-Mail-Adressen an.

Jedes Bedienfeld kann erweitert werden, um verfügbare Optionen anzuzeigen. Standardmäßig ist es platzsparend ausgeblendet (nur das Symbol des Bedienfelds wird angezeigt). Sie können das Bedienfeld erweitern, indem Sie auf das Symbol klicken. Sie können das Bedienfeld wieder ausblenden, indem Sie auf den Pfeil „Ein-/Ausblenden“ oben rechts klicken.

PGP WDE zur Verschlüsselung eines Laufwerks verwenden

Mit der Funktion PGP Whole Disk Encryption (WDE) kann der gesamte Inhalt Ihres Systems oder eines von Ihnen angegebenen externen oder USB-Flash-Laufwerks gesperrt werden.

Der von PGP WDE verwendete Verschlüsselungsalgorithmus ist AES256. Der Hashing-Algorithmus ist SHA-1. Mit FAT16, FAT32 und NTFS formatierte Laufwerke werden unterstützt. Es gibt keine minimale oder maximale Größe. Wenn das Laufwerk vom Betriebssystem (oder dem Hardware-BIOS für das Boot-Laufwerk) unterstützt wird, sollte es mit PGP WDE kompatibel sein.

Achtung: PGP Corporation empfiehlt als beste Praktik, dass Sie vor der Verschlüsselung des Laufwerks Ihre Daten sichern.

- Klicken Sie auf **Gesamte Festplatte verschlüsseln** im Bedienfeld „PGP Disk“.



- Wählen Sie das zu verschlüsselnde Laufwerk bzw. die Partition.
- Wählen Sie **Maximale CPU-Nutzung**, um Ihr Laufwerk so schnell wie möglich zu schützen. Der Verschlüsselungsprozess hat Priorität vor den anderen Betriebsabläufen auf Ihrem System.
- Wählen Sie **Stromausfallschutz**, wenn Sie befürchten, dass während des Verschlüsselungsprozesses ein Stromausfall auftreten könnte.

Bei Auswahl von **Stromausfallschutz** kann der Verschlüsselungsprozess sicher wieder aufgenommen werden,

wenn er unterbrochen wird. Diese Option kann zu einer längeren Ausführungszeit für die Verschlüsselung führen.

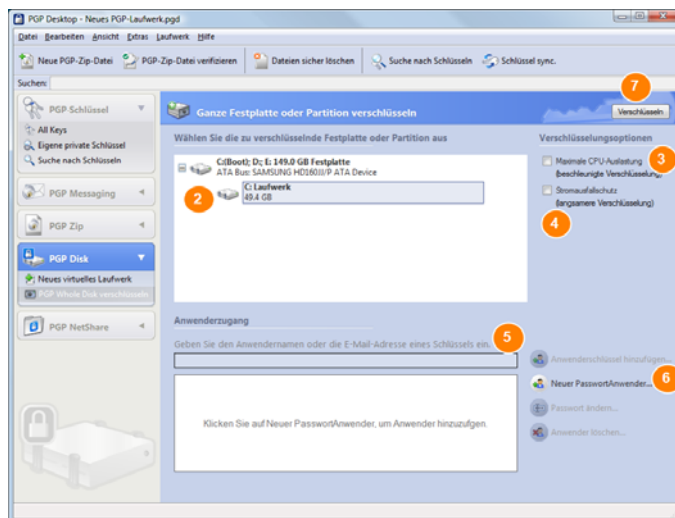
5. Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die die Fähigkeit haben werden, die Authentifizierung für das gesamte verschlüsselte Laufwerk über Kryptographie mit öffentlichem Schlüssel vorzunehmen.

Bei Verschlüsselung einer Festplatte können Sie nur ein PGP-Schlüsselpaar auf einem Aladdin eToken USB-Token verwenden. Bei Verschlüsselung einer Partition oder eines Wechsellaufwerks (keine Festplatte) können Sie jedes Schlüsselpaar auf Ihrem System verwenden.

6. Klicken Sie auf **Neuer Passwort-Anwender**, um Anwender hinzuzufügen, die die Authentifizierung mit einem Passwort vornehmen, oder ein USB-Laufwerk mit zweifaktorieller Authentifizierung verwenden wollen. Folgen Sie der Anleitung, die im Dialogfeld PGP Disk-Assistent angezeigt wird.

Bei Verschlüsselung Ihres Boot-Laufwerks haben Sie die Option, Ihr Passwort zur Anmeldung für Windows zu verwenden, so dass Sie Ihre Anmeldedaten nur einmal beim Systemstart einzugeben brauchen.

7. Klicken Sie auf **Verschlüsseln**.



Hinweise: Zur Verschlüsselung von Daten auf Disketten oder CD-RWs verwenden Sie PGP Virtual Disk-Laufwerke, aber niemals PGP WDE.

Sie können PGP Whole Disk Encryption nur dann mit einem Dual-Boot-System verwenden, wenn Sie das System mit einem Betriebssystem starten, das durch PGP WDE unterstützt wird (zum Beispiel Windows XP, Windows 2000 oder Windows Vista), und PGP Whole Disk Encryption installiert ist. Der Partitionsmodus unterstützt Dual-Boot mit einem anderen Betriebssystem (zum Beispiel Linux) nur dann, wenn Sie nur die Windows-Partition verschlüsseln. Dieses andere Betriebssystem muß sich allerdings auf einer anderen, nicht verschlüsselten Partition befinden.

Sicherungssoftware funktioniert in der Regel mit PGP WDE; alle von der Software gesicherten Dateien werden vor dem

Anlegen der Sicherungskopie entschlüsselt.

PGP WDE - Bewährte Methoden

PGP Corporation empfiehlt die folgenden bewährten Methoden zur Vorbereitung der Verschlüsselung Ihres Laufwerks mit PGP WDE. Bitte befolgen Sie die nachstehenden Empfehlungen zum Schutz Ihrer Daten während und nach der Verschlüsselung.

Vor der Verschlüsselung des Laufwerks müssen Sie einige Schritte ausführen, um die erfolgreiche Erstverschlüsselung des Laufwerks sicherzustellen.

1. **Vergewissern Sie sich, dass Ihr Ziellaufwerk unterstützt wird.** Die PGP WDE-Funktion schützt 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. Siehe „Unterstützte Laufwerktypen“ im *Anwenderhandbuch für PGP Whole Disk Encryption* für weitere Einzelheiten zu den unterstützten Laufwerktypen.
2. **Sichern Sie das Laufwerk, bevor Sie es verschlüsseln.** Sichern Sie das Laufwerk vor der Verschlüsselung, damit keine Daten verloren gehen, wenn der Laptop oder Computer verloren geht, gestohlen wird oder Sie das Laufwerk nicht entschlüsseln können.
3. **Stellen Sie vor dem Verschlüsseln sicher, dass sich das Laufwerk in einwandfreiem Zustand befindet.** Falls PGP WDE während der Verschlüsselung Laufwerksfehler erkennt, hält das Programm an, damit die Probleme behoben werden können. Es ist jedoch effizienter, die Fehlerbehebung vor der Erstverschlüsselung vorzunehmen. Siehe *Einwandfreien Zustand des Laufwerks vor der Verschlüsselung sicherstellen* (Seite 6) für weitere Informationen.
4. **Erstellen Sie einen Wiederherstellungsdatenträger.** Obwohl die Wahrscheinlichkeit äußerst gering ist, dass ein Master-Boot-Datensatz auf einem mit PGP Whole Disk Encryption verschlüsselten Boot-Laufwerk bzw. einer Partition beschädigt wird, kann dies nicht ausgeschlossen werden. Erstellen Sie, bevor Sie ein Laufwerk oder eine Partition mit PGP Whole Disk Encryption verschlüsseln, einen Wiederherstellungsdatenträger. Siehe *Eine Wiederherstellungs-CD erstellen* (Seite 6) für eine Anleitung zur Erstellung eines Wiederherstellungsdatenträgers.
5. **Stellen Sie sicher, dass Ihnen für die Dauer der Verschlüsselung eine Netzstromversorgung zur Verfügung steht.** Siehe *Netzstromversorgung im Verlauf der Verschlüsselung aufrechterhalten* (Seite 6).
6. **Führen Sie einen Versuchstest aus, um die Softwarekompatibilität sicherzustellen.** PGP Corporation empfiehlt als gute Sicherheitspraxis, PGP WDE auf einer kleinen Gruppe von Computern zu testen, um sicherzustellen, dass kein Konflikt zwischen PGP WDE und anderer Software auf dem Computer besteht, bevor es auf einer großen Gruppe von Computern bereitgestellt wird. Das ist besonders nützlich in Umgebungen, die ein

standardisiertes Corporate Operating Environment (COE)-Bild verwenden. Für eine Liste der Software mit bekannten Kompatibilitätsproblemen mit PGP WDE siehe *Ausführung Einen Versuchstest zur Sicherstellung der Softwarekompatibilität ausführen* (Seite 7).

7. **Durchführung einer Laufwerkwiederherstellung auf entschlüsselten Laufwerken.** Wenn Laufwerkwiederherstellungsaktivitäten an einem mit PGP Whole Disk Encryption (WDE) geschützten Wechseldatenträger vorgenommen werden müssen, empfiehlt PGP Corporation als beste Praktik die vorherige Entschlüsselung des Laufwerks. Nehmen Sie das mit Hilfe von **Laufwerk > Entschlüsseln** in PGP Whole Disk Encryption unter Einsatz Ihres vorbereiteten PGP WDE Wiederherstellungsdatenträgers oder durch Anschluss der Festplatte mit einem USB-Kabel an einem zweiten System und Entschlüsselung über die PGP Whole Disk Encryption-Software dieses Systems vor. Setzen Sie die Wiederherstellung nach der Entschlüsselung fort.

Die Laufwerksintegrität vor der Verschlüsselung sicherstellen

PGP Corporation nimmt bewusst eine konservative Haltung bei der Laufwerkverschlüsselung ein, um Datenverlust zu verhindern. Bei der Verschlüsselung von Festplatten treten nicht selten CRC (Cyclic Redundancy Check)-Fehler auf. Wenn PGP WDE eine Festplatte oder Partition mit beschädigten Sektoren feststellt, wird der Verschlüsselungsprozess standardgemäß unterbrochen. Während dieser Pause können Sie das Problem beheben, bevor Sie den Verschlüsselungsprozess fortsetzen, und auf diese Weise mögliche Laufwerkbeschädigung und Datenverlust verhindern.

Um eine Unterbrechung der Verschlüsselung zu verhindern, empfiehlt PGP Corporation, vor der Verschlüsselung alle Laufwerkfehler zu korrigieren, um mit einem Laufwerk mit einwandfreier Integrität zu beginnen.

- Es empfiehlt sich vor dem Versuch, PGP WDE zu verwenden, ein Festplatten-Dienstprogramm eines Drittherstellers zu verwenden. Dieses Dienstprogramm muss die Fähigkeit haben, eine Low-Level-Integritätskontrolle durchzuführen und alle Unregelmäßigkeiten des Laufwerks, die zu CRC-Fehlern führen könnten, zu reparieren. Das Checkdisk-Programm von Disk Microsoft Windows (chkdsk.exe) reicht nicht aus, um diese Probleme auf dem Ziellaufwerk festzustellen. Verwenden Sie stattdessen Software wie SpinRite oder Norton Disk Doctor™. Diese Softwareanwendungen können Fehler korrigieren, die ansonsten die Verschlüsselung unterbrechen würden.
- Es hat sich bewährt, stark fragmentierte Laufwerke vor der Verschlüsselung zu defragmentieren..

Eine Wiederherstellungs-CD erstellen:

Die folgende Anleitung verwendet Roxio-Software für Illustrationszwecke. Die tatsächlich von Ihnen durchgeführten Schritte können abweichend sein.

1. Vergewissern Sie sich, dass PGP Whole Disk Encryption und Roxio Easy Media Creator oder Roxio Easy CD Creator (oder eine andere Software, die eine CD aus einem ISO-Image erstellen kann) auf Ihrem System 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. .
3. Wählen Sie **File (Datei) > Record CD from CD Image (CD über CD-Image aufnehmen)**.
4. Wählen Sie im Menü **Files of Type (Dateityp)** die Option **ISO Image Files (ISO-Image-Dateien)** aus.
5. Navigieren Sie zum PGP-Verzeichnis. Der Standard-speicherort ist C:\Programme\PGP Corporation\PGP Desktop\.
6. Wählen Sie **bootg.iso** aus, und klicken Sie auf **Öffnen**.
7. Legen Sie eine leere, beschreibbare CD in das CD-Laufwerk ein.
8. Klicken Sie im Bildschirm Record CD Setup (CD-Aufzeichnung-Setup) auf **Start Recording (Aufzeichnung starten)**.
9. .
10. Wenn die Datei auf der CD registriert ist, klicken Sie auf **OK**.
11. Nehmen Sie die Wiederherstellungs-CD aus dem Laufwerk, und beschriften Sie sie entsprechend.

Achtung: PGP WDE-Wiederherstellungsdatenträger sind nur mit der Version von PGP Whole Disk Encryption kompatibel, mit der die Wiederherstellungs-CD erstellt wurde. Wenn Sie z. B. versuchen, mit einer in Version 9.0.x erstellten Wiederherstellungs-CD ein durch PGP WDE 9.7 geschütztes Laufwerk zu entschlüsseln, kann nicht mehr auf das PGP WDE 9.7-Laufwerk zugegriffen werden.

Netzbetrieb während der Verschlüsselung beibehalten

Weil die Verschlüsselung ein CPU-intensiver Prozess ist, kann keine Verschlüsselung auf einem Laptop, der im Akkubetrieb angeschlossen ist, gestartet werden. Der Computer *muss* über das Netzteil mit Strom versorgt werden. Wenn Sie einen Laptop während der erstmaligen Verschlüsselung (oder der späteren Entschlüsselung bzw. Umschlüsselung) in den Akkubetrieb umschalten, wird die PGP WDE-Aktivität angehalten. Die Verschlüsselung, Entschlüsselung oder Umschlüsselung wird automatisch fortgesetzt, sobald der Computer wieder über das Netzteil mit Strom versorgt wird.

Unabhängig vom verwendeten Computertyp darf während der Verschlüsselung die Stromversorgung nicht unterbrochen oder das System anderweitig unerwartet herunterfahren werden, sofern Sie nicht die Option „Stromausfallschutz“ ausgewählt haben.

Ziehen Sie das Netzkabel auf keinen Fall ab, bevor der Verschlüsselungsvorgang abgeschlossen ist. Wenn es während

der Verschlüsselung zu einem Stromausfall kommen kann—oder wenn keine unterbrechungsfreie Stromversorgung für Ihren Computer existiert—sollten Sie die Option „Stromausfallschutz“ aktivieren, die im *Anwenderhandbuch für PGP Whole Disk Encryption* beschrieben ist.

Achtung: Dies gilt ebenfalls für Wechseldatenträger, wie zum Beispiel USB-Geräte. Wenn die Option „Stromausfallschutz“ nicht ausgewählt ist, laufen Sie Gefahr, dass das Gerät beschädigt wird, wenn Sie es während der Verschlüsselung entfernen.

Versuchstest zur Sicherstellung der Softwarekompatibilität ausführen

Es gibt andere Arten von Laufwerksschutz-Software, die nicht mit PGP WDE kompatibel sind und schwerwiegende Laufwerkprobleme verursachen können, einschließlich Datenverlust.

Bitte beachten Sie die folgenden bekannten Interoperabilitätsprobleme und lesen Sie die neusten Updates dieser Liste in den PGP Whole Disk Encryption-Versionshinweisen.

Inkompatible Software:

- Faronics Deep Freeze (alle Ausgaben)
- Utimaco Safeguard Easy 3.x.
- CompuTrace Laptop-Sicherheitsprodukt von Absolute Software. PGP Whole Disk Encryption ist nur mit der BIOS-Konfiguration von CompuTrace kompatibel. Die Verwendung von CompuTrace im MBR-Modus ist nicht kompatibel.
- Produkte zur Festplattenverschlüsselung von GuardianEdge Technologies: Dies betrifft die früher unter der Bezeichnung „PC Guardian“ vertriebenen Produkte „Encryption Anywhere Hard Disk“ und „Encryption Plus Hard Disk“.

Die folgenden Anwendungen können mit PGP Whole Disk Encryption auf demselben System installiert werden, blockieren jedoch die Funktion von PGP Whole Disk Encryption:

- Safeboot Solo
- SecureStar SCPP

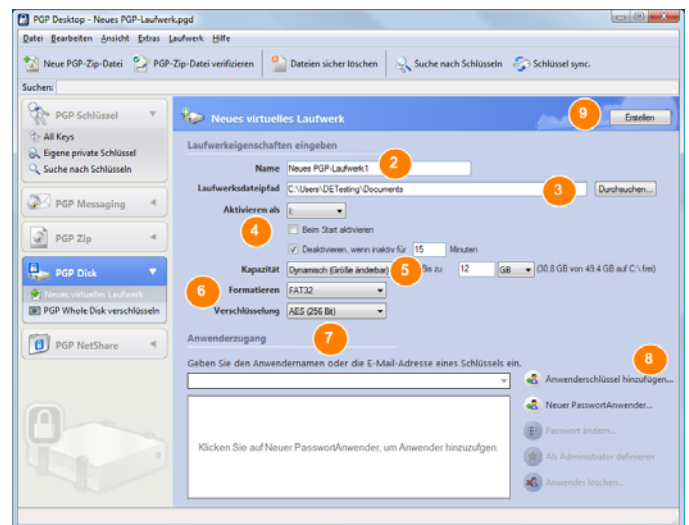
PGP Virtual Disk-Laufwerke erstellen

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

1. Klicken Sie auf **Neues Virtual Disk-Laufwerk** im Bedienfeld „PGP Disk“.

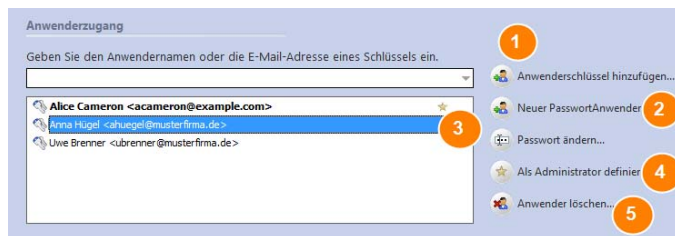


2. Geben Sie einen **Namen** für das Laufwerk ein.
3. Geben Sie einen **Laufwerksdateipfad** für das Laufwerk ein.
4. Geben Sie Ihre Aktivierungspräferenzen wie folgt an:
 - wählen Sie unter **Aktivieren** einen Laufwerksbuchstaben für den Datenträger aus.
 - wählen Sie **Beim Start aktivieren**, damit Ihr neues Laufwerk automatisch beim Start aktiviert wird.
 - wählen Sie **Deaktivieren wenn inaktiv für x Minuten**, wenn das Laufwerk automatisch deaktiviert werden soll, wenn es für die Dauer der angegebenen Minuten inaktiv war.
5. Wählen Sie unter **Kapazität** die Option **Dynamisch (Größe änderbar)**, wenn Sie wollen, dass die Größe des Laufwerks zunimmt, wenn Sie Dateien hinzufügen, oder wählen Sie **Feste Größe**, wenn Sie wollen, dass das Laufwerk immer die gleiche Größe hat.
6. Geben Sie unter **Format** ein Dateisystemformat für das Laufwerk an.
7. Geben Sie unter **Verschlüsselung** einen Verschlüsselungsalgorithmus für das Laufwerk an.
8. Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die die Authentifizierung über Kryptographie mit öffentlichem Schlüssel vornehmen, oder klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die die Authentifizierung mit Passwörtern vornehmen.
9. Klicken Sie auf **Erstellen**.



Verwenden Sie den Abschnitt **Anwenderzugang** zur Kontrolle von bestehenden Benutzern eines PGP Virtual Disk-Laufwerks:

1. Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die die Authentifizierung über Kryptographie mit öffentlichem Schlüssel vornehmen.
2. Klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die die Authentifizierung mit Passwörtern vornehmen.
3. Wählen Sie einen Passwortanwender und klicken Sie dann auf **Passwort ändern**, um sein Passwort zu ändern.
4. Wählen Sie einen Anwender und klicken Sie dann auf **Als Administrator definieren**, um dem Benutzer Administratorrechte zu verleihen.
5. Wählen Sie einen Anwender und klicken Sie dann auf **Löschen**, um ihn zu löschen.



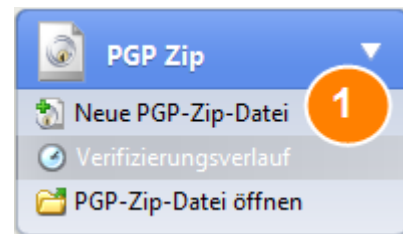
PGP Zip-Archive erstellen

Mit PGP Zip-Archiven können Sie beliebige Kombinationen von Dateien und Ordnern in ein komprimiertes, portables Archiv setzen. Es gibt vier Arten von PGP Zip-Archiven:

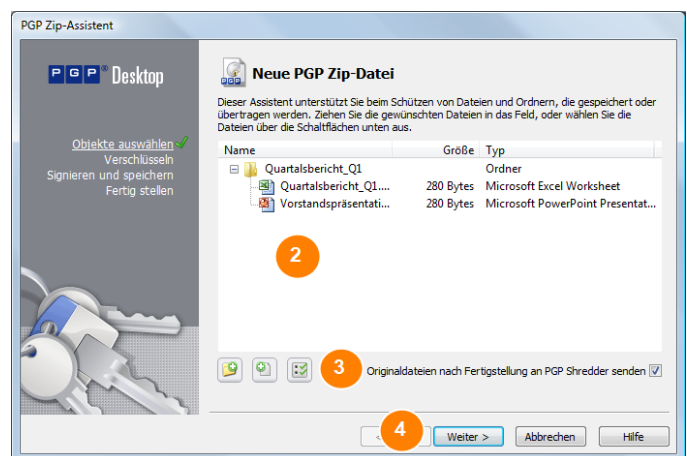
- **Empfängerschlüssel.** Verschlüsselt das Archiv für öffentliche Schlüssel. Nur der Inhaber der entsprechenden privaten Schlüssel kann das Archiv öffnen. Dies ist der sicherste Typ eines PGP Zip-Archivs. Die Empfänger müssen PGP-Software (für Windows oder Mac OS X) benutzen.
- **Passwort.** Verschlüsselt das Archiv für ein Passwort, das den Empfängern mitgeteilt werden muss. Die Empfänger müssen PGP-Software (für Windows oder Mac OS X) verwenden.
- **Selbstentschlüsselndes PGP-Archiv.** Verschlüsselt das Archiv für ein Passwort. Empfänger brauchen keine PGP-Software, um es zu öffnen, aber auf ihren Computern muß Windows oder Mac OS X ausgeführt. Das Passwort muss den Empfängern mitgeteilt werden.
- **Nur signieren.** Signiert das Archiv, ohne es zu verschlüsseln, und ermöglicht Ihnen so den Nachweis, dass Sie der Absender sind. Die Empfänger müssen PGP Whole Disk Encryption oder PGP Desktop oder PGP Desktop für Windows benutzen, um das Archiv öffnen und verifizieren zu können.

Die PGP Zip-Typen „Passwort“ und „Nur signieren“ sind im *Anwenderhandbuch für PGP Desktop* in näheren Einzelheiten beschrieben; sie werden daher hier nur kurz angesprochen.

1. Klicken Sie auf **Neues PGP Zip** im Bedienfeld „PGP Zip“.



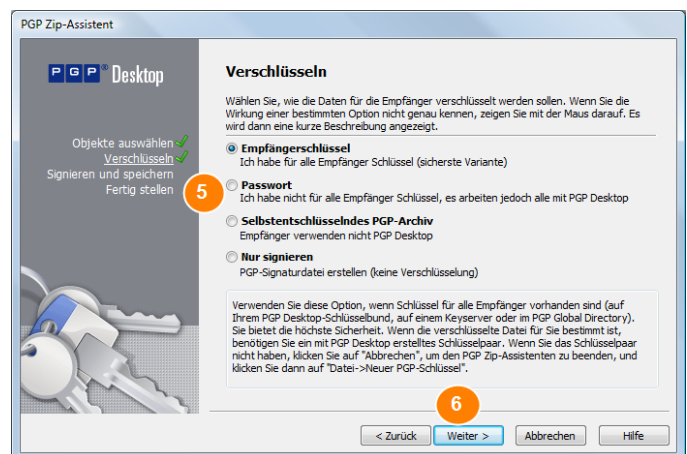
2. Ziehen und legen Sie die gewünschten Dateien/Ordner im Archiv ab oder wählen Sie sie mit Hilfe der Schaltflächen aus.
3. Wählen Sie **Originaldateien nach Fertigstellung an PGP Shredder senden**, wenn Sie wollen, dass die von Ihnen in das Archiv gesetzten Dateien/Ordner nach Erstellung des Archivs sicher gelöscht werden.
4. Klicken Sie auf **Weiter**.



5. Wählen Sie den gewünschten Typ des PGP Zip-Archivs:

- **Empfängerschlüssel**
- **Passwort**
- **Selbstentschlüsselndes PGP-Archiv**
- **Nur signieren**

6. Klicken Sie auf **Weiter**.



Die Typen **Passwort** und **Nur signieren** sind im Benutzer-

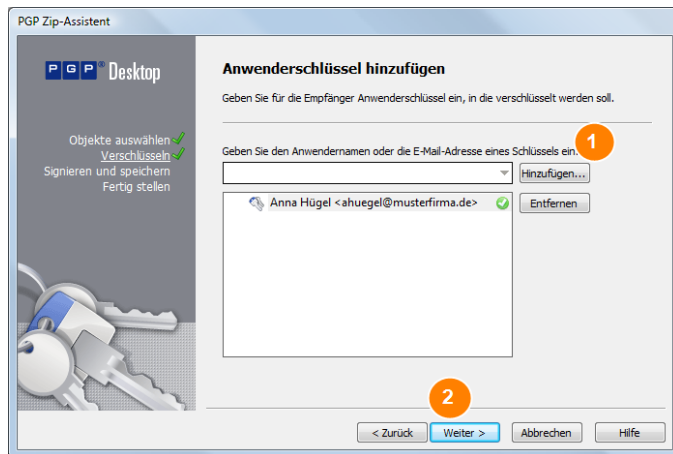
handbuch für *PGP Desktop* in näheren Einzelheiten beschrieben.

Beziehen Sie sich auf den entsprechenden Abschnitt auf den folgenden Seiten für Informationen zum von Ihnen angegebenen PGP Zip-Archivtyp.

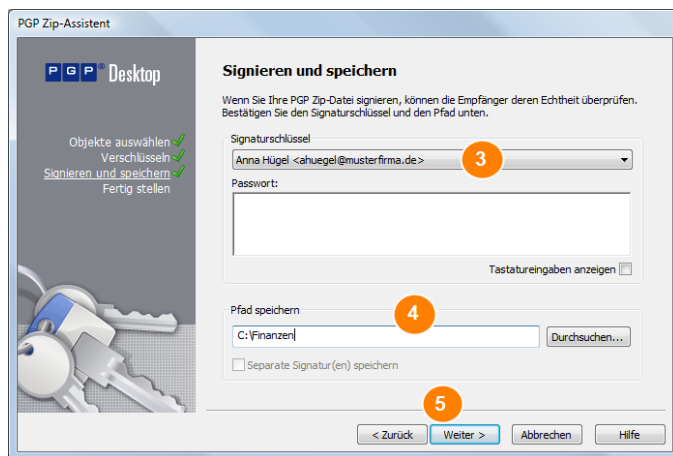
Empfängerschlüssel

Der Bildschirm „Anwenderschlüssel hinzufügen“ erscheint.

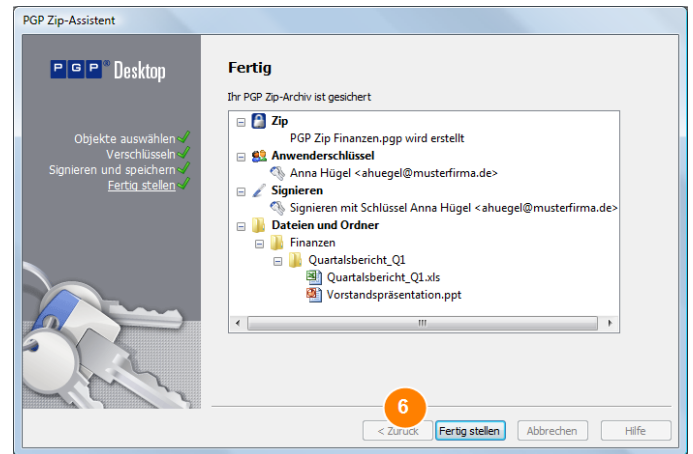
1. Klicken Sie auf **Hinzufügen** und verwenden Sie den Bildschirm „Anwenderauswahl“, um die öffentlichen Schlüssel der Personen auszuwählen, die Sie zur Öffnung des Archivs befähigen wollen. Damit Sie das Archiv auch selbst öffnen können, müssen Sie auch Ihren öffentlichen Schlüssel mit aufnehmen.
2. Klicken Sie auf **Weiter**.



3. Wählen Sie einen privaten Schlüssel auf dem lokalen System, den Sie zur Signatur des Archivs verwenden.
4. Geben Sie einen Namen und einen Speicherort für das Archiv an. Der Standardname ist der Name der ersten Datei bzw. Ordners im Archiv; der Standardspeicherort ist der Speicherort der Dateien/Ordner, die in das Archiv gesetzt werden.
5. Klicken Sie auf **Weiter**. Das PGP Zip-Archiv wird erstellt. Der Bildschirm „Beendet“ zeigt Informationen über das neue Archiv an.



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



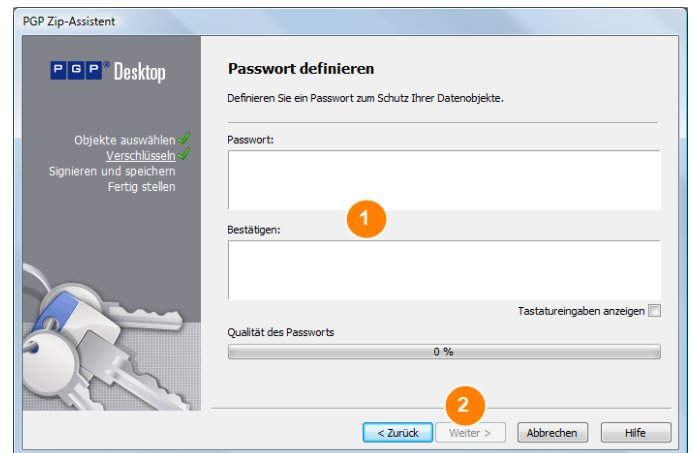
Hinweis: Der Passwort-Typ des PGP Zip-Archivs ist dem Typ Empfängerschlüssel sehr ähnlich; der einzige Unterschied ist, dass ein Passwort statt eines Schlüssels zum Schutz des Archivs verwendet wird.

Hinweis: Der Typ „Nur signieren“ des PGP Zip-Archivs ist dem Typ Empfängerschlüssel sehr ähnlich; der einzige Unterschied ist, dass Sie keine öffentlichen Schlüssel auswählen, weil das Archiv lediglich signiert, jedoch nicht verschlüsselt wird.

Selbstentschlüsselndes PGP-Archiv

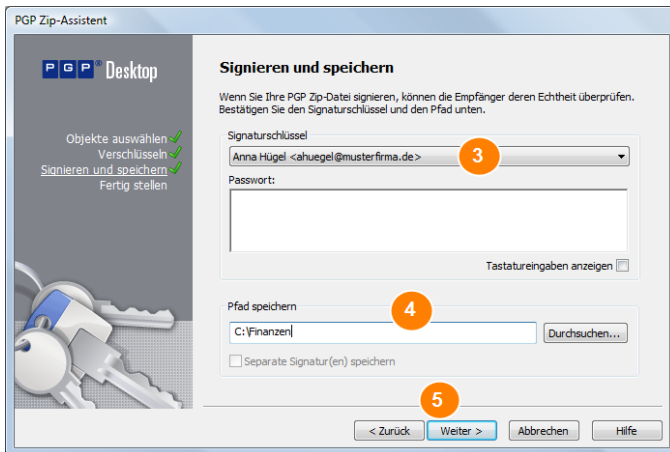
Der Bildschirm „Passwort definieren“ wird geöffnet.

1. Geben Sie ein Passwort für das PGP Zip Selbstentschlüsselnde Archiv (SDA) ein und bestätigen Sie es, indem Sie es erneut eingeben.
2. Klicken Sie auf **Weiter**.

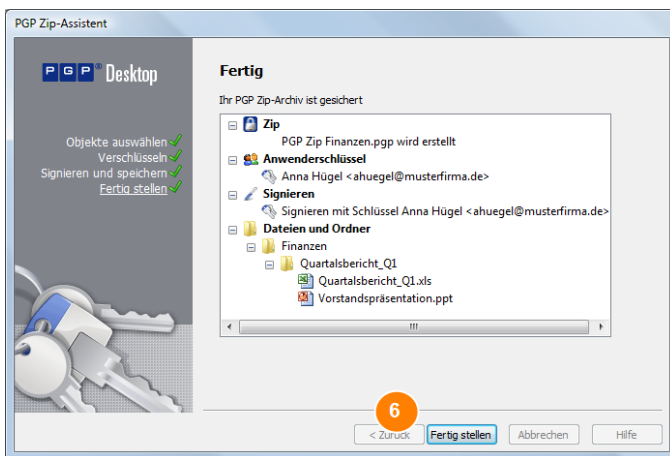


3. Wählen Sie einen privaten Schlüssel auf dem lokalen System, den Sie zur Signatur des Archivs verwenden.
4. Geben Sie einen Namen und einen Speicherort für das Archiv an. Der Standardname ist der Name der ersten Datei bzw. Ordners im Archiv; der Standardspeicherort ist der Speicherort der Dateien/Ordner, die in das Archiv gesetzt werden.

5. Klicken Sie auf **Weiter**. Das PGP SDA wird erstellt.



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



PGP Shred zur sicheren Löschung von Dateien verwenden

Die Funktion PGP Shredder vernichtet Dateien und Ordner vollständig, so dass sie selbst mit hochentwickelter Dateiwiederherstellungssoftware nicht wiederhergestellt werden können. Obwohl das PGP Shredder-Symbol wie auch der Windows-Papierkorb auf Ihrem Desktop erscheinen, werden die angegebenen Dateien nur von PGP Shredder sofort überschrieben, so dass sie nicht wiederherstellbar sind.

Die sichere Löschung von Dateien ist mit jedem der folgenden Verfahren möglich:

- Über das PGP Shredder-Symbol
- Über die PGP-Symboleiste
- Über das PGP-Kontextmenü

Dateien mit dem PGP Shredder-Symbol sicher löschen

➤ So löschen Sie Dateien mit dem PGP Shredder-Symbol sicher

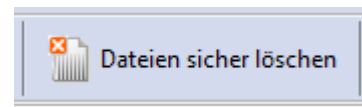
1. Ziehen Sie auf dem Windows-Desktop die Dateien und Ordner, die Sie sicher löschen wollen, in den PGP Shredder. Im nun erscheinenden Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Dateien sicher löschen wollen.
2. Klicken Sie auf **Ja**. Die angegebenen Dateien und Ordner werden nun sicher gelöscht.



Dateien mit der PGP-Symboleiste sicher löschen

➤ So löschen Sie Dateien mit der PGP-Symboleiste sicher

1. Öffnen Sie PGP Whole Disk Encryption.
2. Klicken Sie auf **Dateien sicher löschen** auf der PGP-Symboleiste.
3. Geben Sie die Dateien an, die Sie sicher löschen wollen. Klicken Sie bei gedrückter STRG-Taste, um mehrere Dateien auszuwählen, oder markieren Sie mit STRG-A alle angezeigten Dateien.
4. Klicken Sie auf **Öffnen**. Im nun erscheinenden Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Dateien sicher löschen wollen.
5. Klicken Sie auf **Ja**. Die angegebenen Dateien und Ordner werden nun sicher gelöscht.



Dateien mit dem PGP Kontextmenü sicher löschen

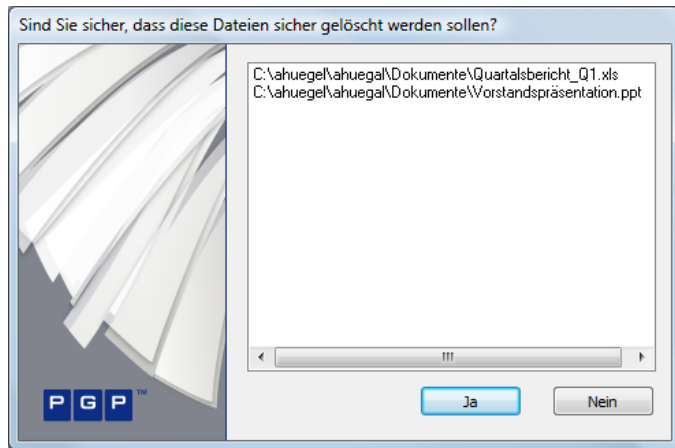
➤ So löschen Sie Dateien sicher in Windows Explorer

1. Öffnen Sie Windows Explorer.
2. Rechtsklicken Sie auf die Dateien oder Ordner, die Sie sicher löschen wollen und wählen Sie dann **PGP Desktop > PGP Shred <Dateiname>**. Klicken Sie bei gedrückter STRG-Taste, um mehrere Dateien auszuwählen, oder markieren Sie mit STRG-A alle angezeigten Dateien.

Tipp: Wenn Sie mehr als eine Datei ausgewählt haben, erscheint der Text **PGP Shred x Objekte**, wobei **x** die Anzahl der ausgewählten Dateien ist.

Im nun erscheinenden Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Dateien sicher löschen wollen.

3. Klicken Sie auf **Ja**. Die angegebenen Dateien und Ordner werden nun sicher gelöscht.



Hinweis: Wenn Sie die Funktion PGP Shredder nicht oft benutzen, können Sie das PGP Shredder-Symbol vom Desktop mit PGP-Optionen entfernen. Wählen Sie **Extras > Optionen** aus, klicken Sie auf die Registerkarte „Laufwerk“, deselektieren Sie die Option **PGP Shredder-Symbol auf dem Desktop platzieren** und klicken Sie dann auf **OK**.

Hinweis: Sie können auch die PGP-Optionen verwenden, um die Anzahl der bei der sicheren Löschung vorgenommenen Durchgänge zu steuern (mehrere Durchgänge sind sicherer, dauern jedoch länger). Sie können hier auch angeben, ob die Dateien im Windows-Papierkorb bei der Leerung sicher gelöscht werden sollen und ob das Warndialogfeld erscheinen soll, wenn Sie die sichere Löschung vornehmen.

Freien Speicherplatz sicher löschen

Die Funktion PGP Shred Free Space (Freien Speicherplatz sicher löschen) löscht freien Speicherplatz auf Ihren Laufwerken, so dass Ihre gelöschten Daten definitiv nicht wiederherstellbar sind. Es ist zu beachten, dass „freier Speicherplatz“ eigentlich eine falsche Bezeichnung ist. PGP Shred Free Space überschreibt die Teile Ihrer Festplatte, die Windows für leer hält; der Speicherplatz kann jedoch leer sein oder Dateien umfassen, die nach Angabe von Windows gelöscht wurden.

Wenn Sie Dateien in den Windows-Papierkorb ablegen und ihn leeren, werden die Dateien nicht wirklich gelöscht; Windows tut nur so, als ob sich dort nichts befindet und überschreibt die Dateien schließlich. Aber bis diese Dateien überschrieben werden, können sie leicht von einem Angreifer wiederhergestellt werden. PGP Shred Free Space überschreibt jedoch diesen „freien Speicherplatz“, so dass diese Dateien selbst mit Wiederherstellungssoftware nicht wieder-

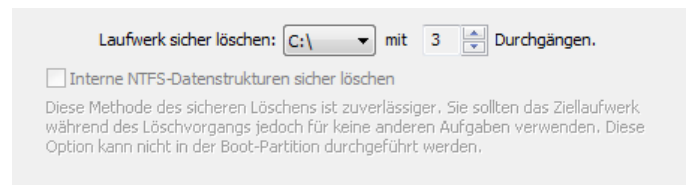
hergestellt werden können.

➤ So löschen Sie sicher freien Speicherplatz auf Ihren Laufwerken

1. Öffnen Sie PGP Whole Disk Encryption.
2. Wählen Sie **Extras > Freien Speicherplatz sicher löschen**.
3. Lesen Sie die einführenden Informationen und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Feld **Laufwerk sicher löschen**, auf dem Bildschirm „Informationen sammeln“, das Laufwerk oder den Datenträger, das bzw. den Sie sicher löschen wollen, sowie die Anzahl der Durchgänge, die PGP Shred für freien Speicherplatz ausführen soll.

Die empfohlenen Richtlinien für Durchgänge sind:

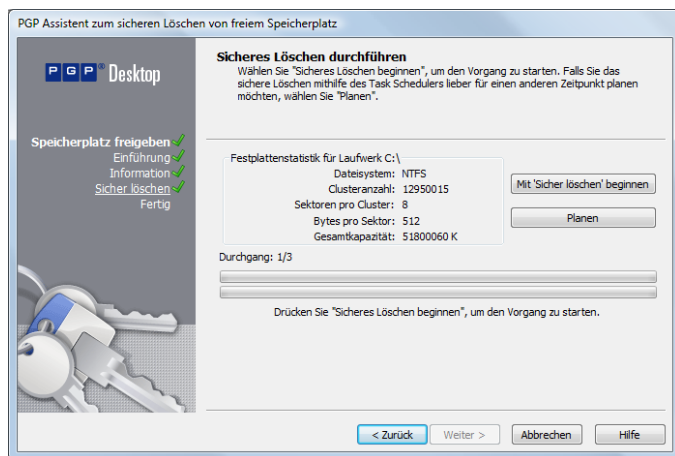
- 3 Durchgänge für den persönlichen Gebrauch.
- 10 Durchgänge für den geschäftlichen Gebrauch.
- 18 Durchgänge für den militärischen Gebrauch.
- 26 Durchgänge für maximale Sicherheit.



5. Wählen Sie ggf. die Option **Interne NTFS-Datenstrukturen sicher löschen** (nicht auf allen Systemen verfügbar) und klicken Sie dann auf **Weiter**. Diese Option löscht sicher kleine Dateien (unter 1KB) in internen Datenstrukturen, die anderenfalls nicht sicher gelöscht werden würden.
6. Klicken Sie auf dem Bildschirm „Sicheres Löschen durchführen“ auf **Sicheres Löschen beginnen**.

Hinweis: Klicken Sie auf **Planen**, wenn Sie einen Zeitpunkt für die sichere Löschung Ihres freien Speicherplatzes ansetzen wollen, anstatt diese jetzt durchzuführen. Der Windows-Taskplaner muss dazu auf Ihrem System installiert sein.

Die Dauer des sicheren Löschsens hängt von der Anzahl der angegebenen Durchgänge, der Geschwindigkeit der CPU, der Anzahl der ausgeführten anderen Anwendungen usw. ab.



7. Klicken Sie nach Abschluss des sicheren Löschens auf **Weiter**.
8. Klicken Sie auf dem Bildschirm „Abschließen“ auf **Beenden**.

Hilfe und Support

Kontaktaufnahme mit dem technischen Support

- Wenn Sie sich über die PGP-Supportoptionen informieren oder Kontakt mit dem technischen Support der PGP Corporation aufnehmen möchten, besuchen Sie bitte die *PGP Corporation Support Home Page* <http://www.pgp.com/support>
- Auf der Website des *PGP Support-Portals* (<https://support.pgp.com>) können Sie auf die PGP Support-Wissensdatenbank zugreifen und PGP Technical Support anfordern. **Beachten Sie, dass Sie bestimmte Teile der PGP Support Knowledge Base ohne Support-Vertrag nutzen können; der technische Support kann Ihre Anfrage jedoch nur bearbeiten, wenn ein gültiger Supportvertrag besteht.**
- Alle weiteren Kontaktinformationen für PGP Corporation finden Sie auf der *PGP Kontakt-Seite* (<http://www.pgp.com/company/contact/index.html>).
- Allgemeine Informationen über die PGP Corporation finden Sie auf der PGP-Website (<http://www.pgp.com>).
- Über die PGP Support-Website können Sie auf die *PGP Support-Foren* zugreifen (<http://forums.pgpsupport.com>). Hierbei handelt es sich um Support-Foren der Anwendergemeinschaft, die von der PGP Corporation gehostet werden.

Verfügbare Dokumentation

Vor der Installation können Sie auf die vollständige Produktdokumentation über die *PGP Support-Wissensdatenbank* zugreifen (<https://support.pgp.com/?faq=589>).

Die PGP Whole Disk Encryption-Dokumentation wird während der Installation auf Ihrem Rechner installiert. Um sie

anzuzeigen, wählen Sie **Start > Programme > PGP > Dokumentation**. Alle Dokumente werden im PDF-Format (Adobe Acrobat Portable Document Format) gespeichert. Diese Dateien können mit Adobe Acrobat Reader, der auf der *Adobe-Website* (<http://www.adobe.com>) abrufbar ist, angezeigt und ausgedruckt werden. PGP Whole Disk Encryption umfasst auch eine integrierte Windows-Onlinehilfe.

Copyright

Copyright © 1991-2009 PGP Corporation. Alle Rechte vorbehalten. „PGP“, „Pretty Good Privacy“ und das PGP-Logo sind in den Vereinigten Staaten von Amerika und anderen Ländern registrierte Warenzeichen der PGP Corporation. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind Eigentum ihrer jeweiligen Eigentümer.