

Was ist PGP NetShare?

PGP NetShare ist eine Sicherheitslösung, die mehrere Möglichkeiten für den Schutz und die Freigabe Ihrer Daten bietet.

Sie können mit PGP NetShare folgende Aufgaben ausführen:

- Anwenden die Freigabe geschützter Dateien in einem freigegebenen Speicherbereich ermöglichen, z. B. auf einem Dateiserver, in einem freigegebenen Ordner oder auf einem USB-Wechsellaufwerk.
- Einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit eigenem Laufwerksbuchstaben verwenden.
- Sichere, verschlüsselte 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 NetShare oder PGP Desktop nicht installiert ist.
- Dateien und Ordner vollständig zerstören, so dass sie selbst mit Datenwiederherstellungssoftware nicht wiederhergestellt werden können.
- Freien Speicherplatz auf Laufwerken sicher löschen, so dass die gelöschten Daten keinesfalls wiederhergestellt werden können.

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 NetShare. Nutzen Sie ihn als Anleitung bei den ersten Schritten mit PGP NetShare und den anderen Sicherheitsmerkmalen im Lieferumfang von PGP Desktop.
- Das *PGP Desktop Anwenderhandbuch* enthält ausführlichere Informationen über PGP NetShare. 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.



Eine PGP NetShare-Lizenz ermöglicht Ihnen den Zugang zu einem bestimmten Teil der Funktionen von PGP Desktop. Für andere Funktionen von PGP Desktop ist ggf. eine andere Lizenz erforderlich. Weitere Informationen finden Sie im Abschnitt zur Lizenzierung im *PGP Desktop Anwenderhandbuch*.

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

Inhalt

■ Was ist PGP NetShare?	1
■ Neu bei PGP Desktop?	1
■ Systemanforderungen	1
■ Was wird installiert?	2
■ Die Grundlagen	2
■ PGP NetShare installieren	4
■ Der PGP NetShare-Hauptbildschirm	5
■ PGP NetShare verwenden	6
■ PGP Virtual Disk-Laufwerke erstellen	7
■ PGP Zip-Archive erstellen	8
■ Dateien sicher löschen	11
■ Freien Speicherplatz sicher löschen	12
■ Weitere Informationen	13

Verwendete Symbole



Hinweis



Achtung

Systemanforderungen

- Windows Vista, Windows XP (SP 1 oder 2), Windows 2000 (SP 4) und Windows 2003 Server (SP 1)
- 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 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.

In PGP NetShare 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 NetShare oder 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 NetShare 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 NetShare 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.

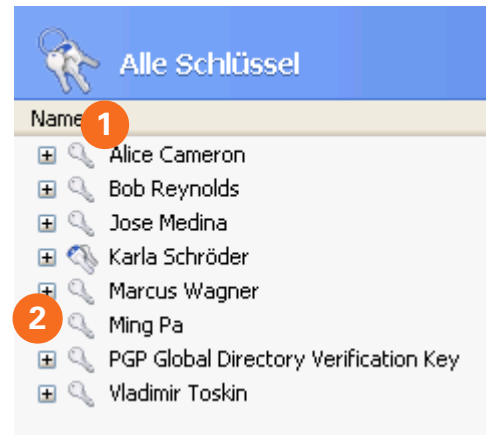
Die Grundlagen

Nach der Installation von PGP NetShare 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 NetShare installieren

Für die Installation ist ein Neustart des Systems erforderlich.

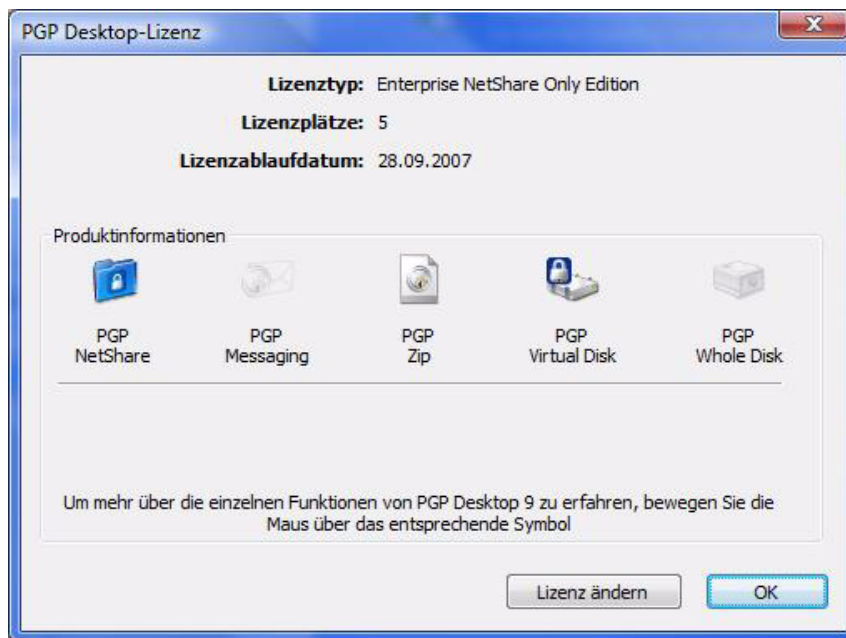
Die PGP Corporation empfiehlt, alle geöffneten Anwendungen vor Beginn der Installation zu beenden.



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

So installieren Sie PGP NetShare:

- 1 Navigieren Sie zum Installationsprogramm für PGP NetShare.
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 NetShare.



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

PGP NetShare starten

Sie können PGP NetShare 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**.

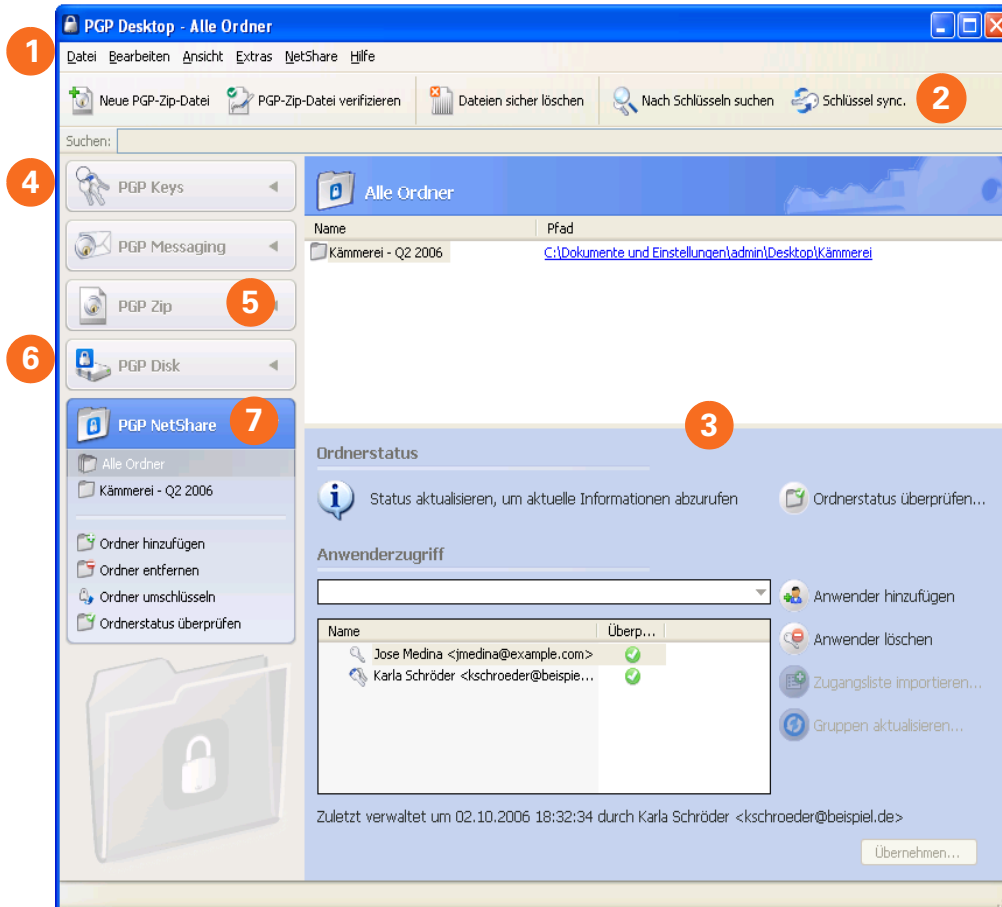


PGP Tray-Symbol

Der PGP NetShare-Hauptbildschirm

Am einfachsten erfolgt der Zugriff auf die Funktionen von PGP NetShare über den Hauptbildschirm.

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



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

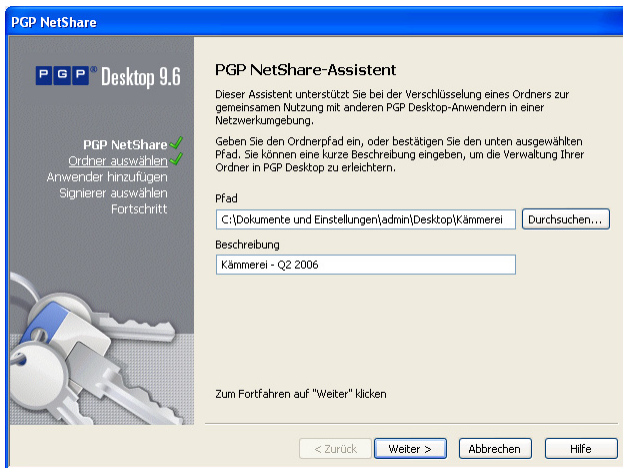
PGP NetShare verwenden

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**.

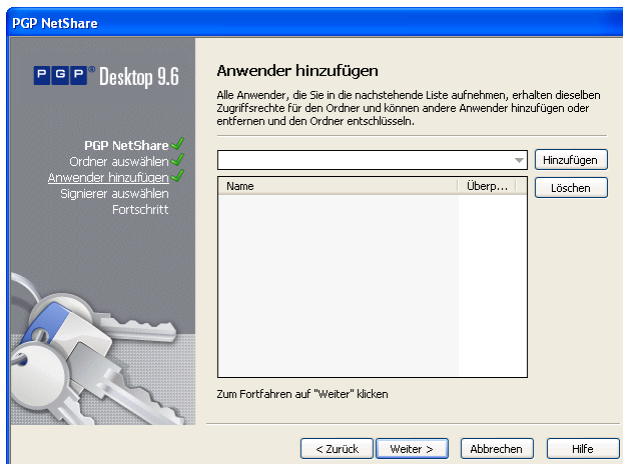


Das Fenster **Ordner auswählen** wird angezeigt.



- 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.



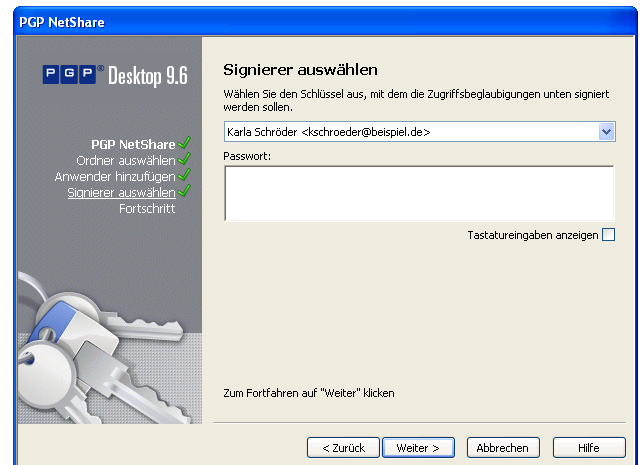
- 5 Klicken Sie auf den Pfeil nach unten, wählen Sie einen Anwender aus, und klicken Sie auf **Hinzufügen**, um die berechtigten Anwender für die Dateien im geschützten Ordner anzugeben.

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

- i** 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.

- 6 Klicken Sie auf **Weiter**.

Das Fenster **Signierer auswählen** wird angezeigt.

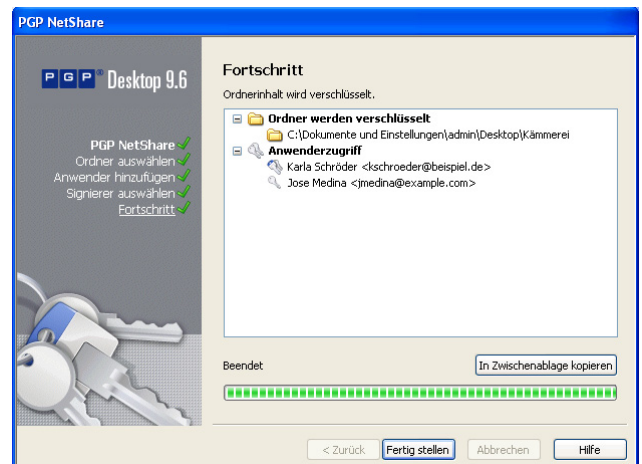


- 7 Wählen Sie einen der privaten Schlüssel am lokalen Schlüsselbund aus, und geben Sie das zugehörige Passwort ein (falls dieses nicht zwischengespeichert ist).

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

- 8 Klicken Sie auf **Weiter**.

Der Bildschirm **Fortschritt** wird angezeigt.



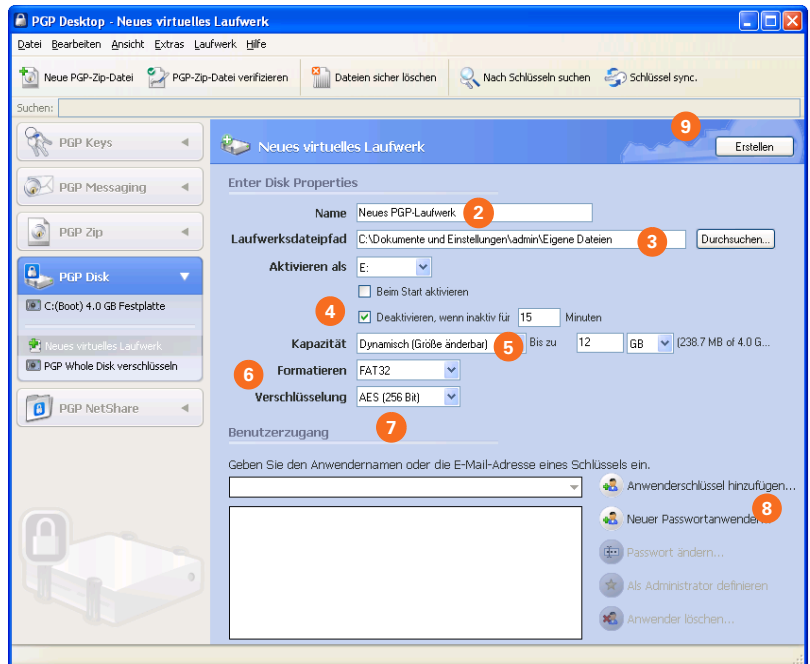
Die Dateien im geschützten Ordner werden verschlüsselt, und die angegebenen Anwender erhalten die Berechtigung zur Verwendung der Dateien.

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

PGP Virtual Disk-Laufwerke erstellen

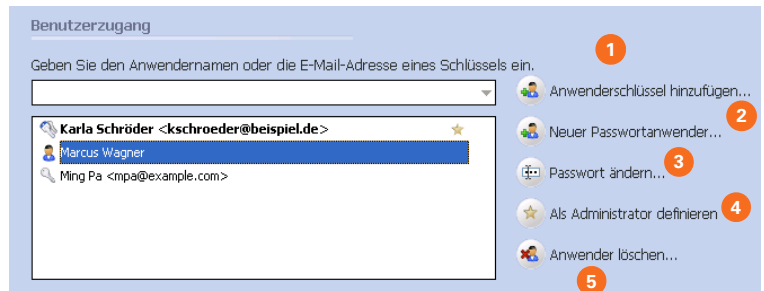
Die Funktion für PGP Virtual Disk-Laufwerke verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit eigenem Laufwerksbuchstaben. Sie können weitere Anwender für ein Laufwerk erstellen und dadurch den autorisierten Personen den Zugriff gestatten.

- 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 **Anwenderzugriff** 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 Zip-Archive erstellen

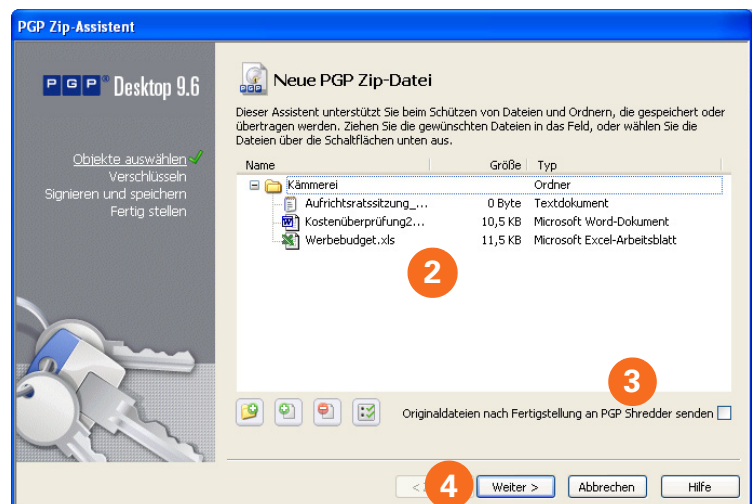
PGP Zip-Archive ermöglichen es Ihnen, beliebige Kombinationen von Dateien und Ordnern in ein komprimiertes und portables Archiv einzufügen. Es gibt vier Arten von PGP Zip-Archiven:

- **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 NetShare oder PGP Desktop für Windows verwenden.
- **Passwort.** Verschlüsselt das Archiv mit einem Passwort, das den Empfängern mitgeteilt werden muss. Die Empfänger müssen PGP NetShare oder PGP Desktop für Windows verwenden.
- **Selbstentschlüsselndes PGP-Archiv.** Verschlüsselt das Archiv mit einem Passwort, die Empfänger benötigen aber *nicht* PGP NetShare 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 NetShare 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.

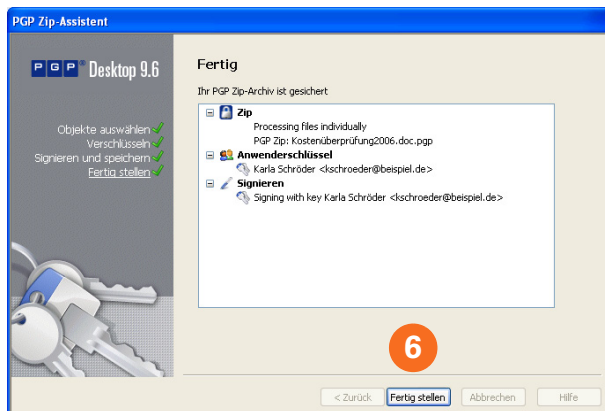
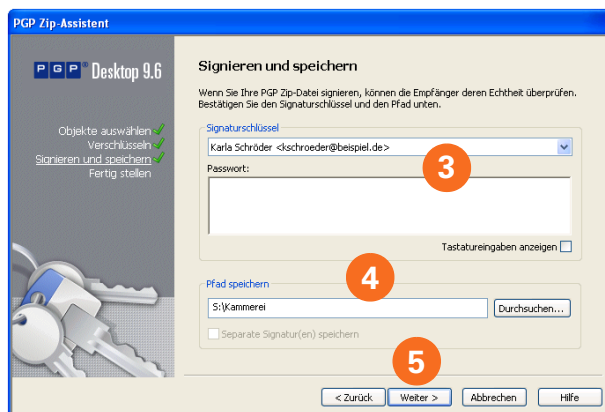
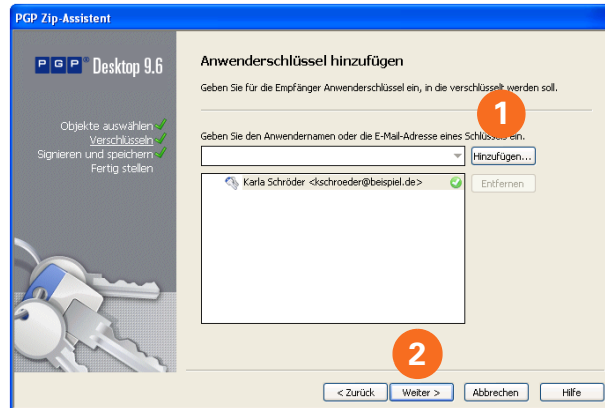
- 6 Klicken Sie auf **Fertig stellen**.



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.

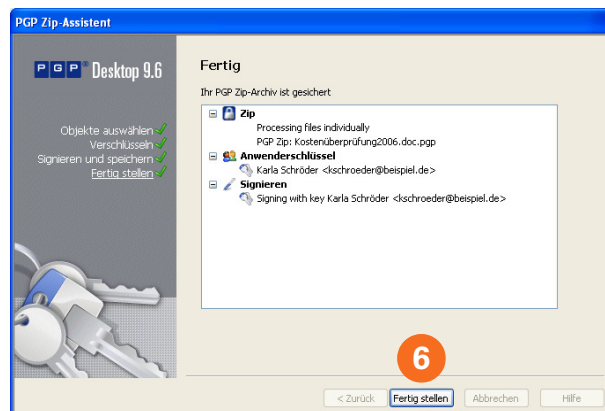
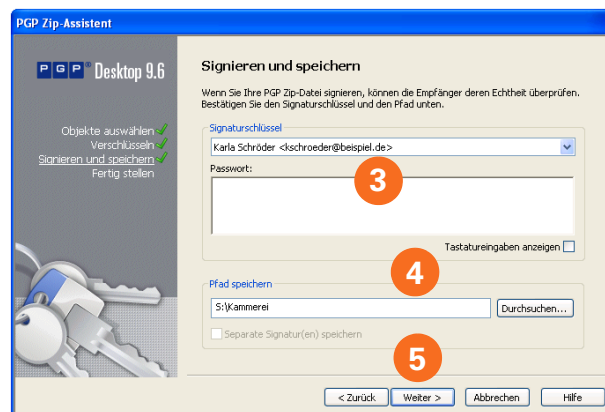
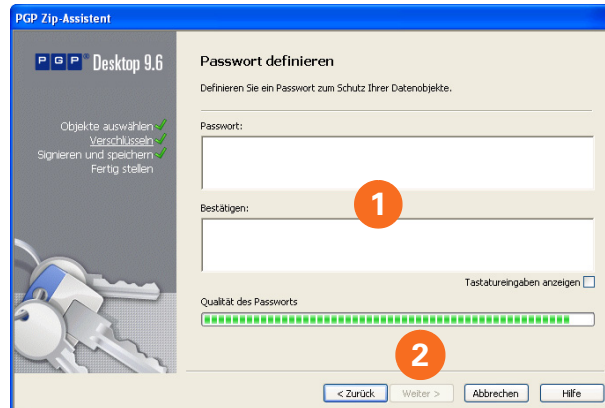
- 4 Legen Sie einen Namen und einen Speicherort für das Archiv fest.

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

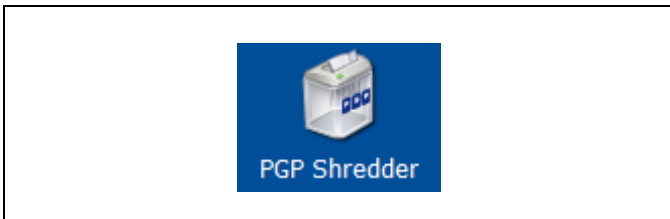
So löschen Sie Dateien sicher mit dem PGP Shred-Symbol:

- 1 Ziehen Sie auf dem Windows-Desktop die Dateien und Ordner, die sicher gelöscht werden sollen, 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 Klicken Sie auf der PGP-Symbolleiste auf **Dateien sicher löschen**.

- 2 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.

- 3 Klicken Sie auf **Öffnen**.

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

- 4 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>**.

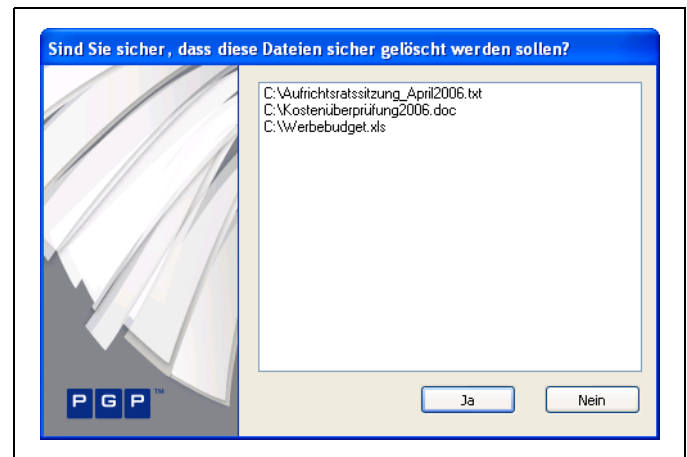
Klicken Sie bei gedrückter Strg-Taste auf die Dateien, um mehrere Dateien auszuwählen, oder drücken Sie Strg+A, um alle angezeigten Dateien auszuwählen.

Wenn Sie mehrere Dateien ausgewählt haben, lautet der Text: **Sicheres Löschen von**, 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.

Weitere Ansprechpartner der PGP Corporation finden Sie im Abschnitt mit Kontakten auf der PGP-Website: **www.pgp.com/company/contact.html**.