



## Was ist PGP Desktop Email?

PGP Desktop Email ist ein Teil der Familie der PGP Desktop-Produkte. Mit PGP Desktop Email können Sie 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 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 Desktop Email?* (Seite 1)
- *Neu bei PGP Desktop Email?* (Seite 1)
- *Die Grundlagen* (Seite 1)
- *Was wird installiert?* (Seite 2)
- *Systemvoraussetzungen* (Seite 3)
- *PGP Email installieren* (Seite 3)
- *PGP Desktop Email starten* (Seite 3)
- *Der Hauptbildschirm von PGP Desktop Email* (Seite 4)
- *PGP Email verwenden* (Seite 4)
- *PGP Virtual Disk-Laufwerke erstellen* (Seite 6)
- *Ein PGP Zip-Archiv erstellen* (Seite 7)
- *Dateien sicher löschen* (Seite 9)
- *Freien Speicherplatz sicher löschen* (Seite 10)
- *Hilfe und Support* (Seite 11)

## Neu bei PGP Desktop Email?

Diese schrittweise Anleitung erleichtert Ihnen den Einstieg. Sie werden feststellen, dass der Schutz Ihrer Daten mit PGP Desktop Email so einfach ist wie das Drehen eines Schlüssels in einem Schloss.

- Dieser *Schnelleinstieg* enthält die Installationsanleitung für PGP Desktop Email und erste Schritte.
- Das *PGP Desktop Email Anwenderhandbuch* stellt noch detailliertere Informationen zu PGP Desktop Email 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 PGP Desktop Email-Lizenz gibt Ihnen Zugang zu einem bestimmten Satz von PGP Desktop Email-Funktionen. Manche anderen Funktionen von PGP Desktop Email können eine andere Lizenz erfordern. Nähere Informationen finden Sie im Abschnitt über Lizenzen im *Anwenderhandbuch für PGP Desktop Email*.

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

## Die Grundlagen

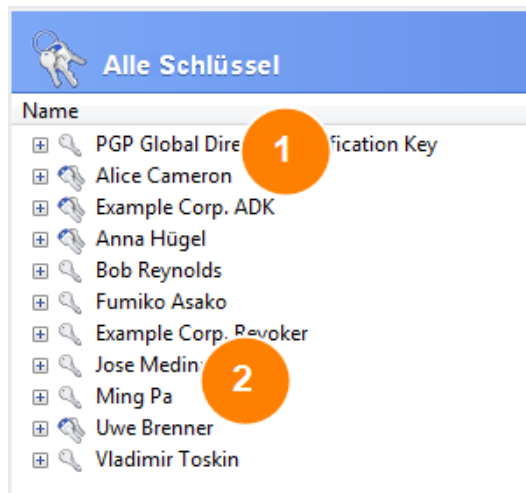
Nach der Installation werden Sie von PGP Desktop Email zur Erstellung eines PGP-Schlüsselpaars aufgefordert. Ein Schlüsselpaar ist die Kombination eines privaten Schlüssels und eines öffentlichen Schlüssels.

- 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 Bedienfeld „PGP Keys“, 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.

2. 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 Desktop Email verwendet Lizenzen, um Zugang zu den von Ihnen erworbenen Funktionen bereitzustellen. Je nach Lizenz können einige oder alle Anwendungen der PGP Desktop Email-Produktfamilie genutzt werden.

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



**PGP Desktop Email** ist eine Anwendung der PGP Desktop-Produktfamilie. PGP Desktop Email kann zur automatischen und transparenten Verschlüsselung, Signatur, Entschlüsselung und Verifikation von E-Mail-Nachrichten mit Richtlinien, über die Sie Kontrolle haben, verwendet werden. PGP Desktop Email kann auch zur Verschlüsselung von IM-Sitzungen für Clients, zum Beispiel AIM und iChat, verwendet werden. Bei beiden Benutzern muss PGP Desktop Email aktiviert sein.

Zu den weiteren Komponenten von PGP Desktop Email gehören:



### PGP Virtual Disk-Laufwerke —

Verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit seinem eigenen Laufwerksbuchstaben. Ein PGP Virtual Disk-Laufwerk 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 vertraulichen Daten zum Zwecke der Verteilung an andere oder Datensicherung.

### Selbstentschlüsselnde PGP-Archive (SDAs) —

Platziert Dateien und Ordner in ein verschlüsseltes, komprimiertes Paket, das auch 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 Dateiwiederherstellungsssoftware 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 Laufwerkswiederherstellungsssoftware 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 Desktop Email 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 zugesandt werden, sowie zur Sicherung Ihrer PGP Virtual Disk-Datenträger. Öffentliche Schlüssel werden zur Verschlüsselung von Nachrichten für andere Personen oder zum Hinzufügen von Benutzern zu PGP Virtual Disk-Datenträgern verwendet.

## Systemvoraussetzungen

- Microsoft Windows 2000 (Servicepack 4), Windows Server 2003 (Servicepack 1), Windows XP (Servicepack 1, 2 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.

- 512 MB RAM
- 64 MB Festplattenspeicher

## PGP Desktop Email installieren

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

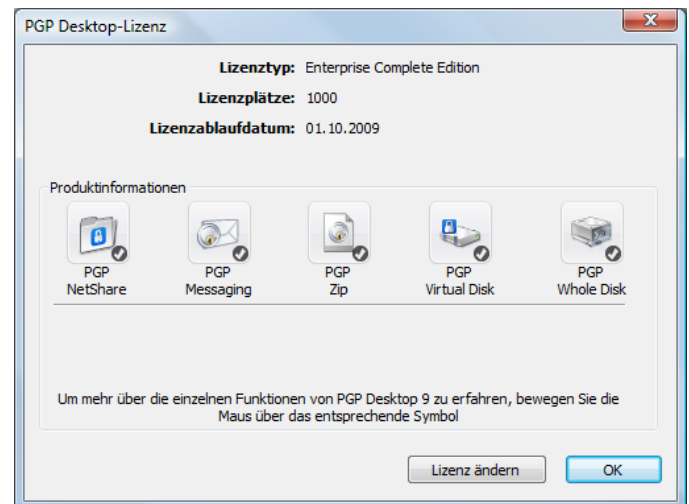
**Hinweis:** Wenn Sie PGP Desktop Email in einer mit PGP Universal Server verwalteten Umgebung verwenden ist Ihre PGP Desktop Email-Installationssoftware möglicherweise mit spezifischen Funktionen und/oder Einstellungen konfiguriert.

### ➤ So installieren Sie PGP Desktop Email

1. Suchen Sie das PGP Desktop Email-Installationsprogramm, das Sie heruntergeladen haben.  
Das Installationsprogramm wurde möglicherweise von Ihrem PGP-Verwalter 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 Desktop Email.

## Lizenzierung

Zur Anzeige der Funktionen, die im Rahmen Ihrer PGP-Lizenz unterstützt werden, öffnen Sie PGP Desktop Email und wählen Sie **Hilfe > Lizenz**. Die Funktionen mit einer Kontrollmarkierung werden von der aktiven Lizenz unterstützt.



## PGP Desktop Email starten

Sie können PGP Desktop Email auf folgende Arten starten:

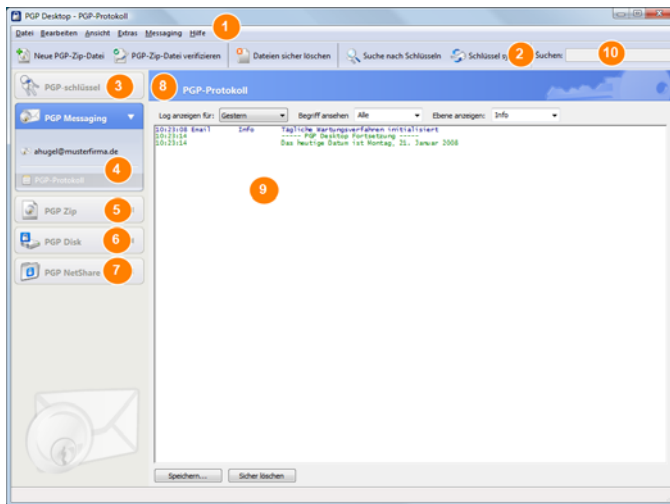
- Doppelklicken Sie auf das PGP Tray-Symbol.



- Rechtsklicken Sie auf das PGP Tray-Symbol und wählen Sie dann **PGP Desktop Email öffnen**.
- Wählen Sie im **Start-Menü Programme > PGP > PGP Desktop Email**.

## Der PGP Desktop Email-Hauptbildschirm

Das Anwendungsfenster von PGP Desktop Email ist die primäre Benutzeroberfläche für das Produkt.



Der PGP Desktop Email-Bildschirm enthält folgende Elemente:

- 1 Menüleiste.** Ermöglicht den Zugriff auf PGP Desktop Email-Befehle. 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 Desktop Email.** Hier werden neben verschiedenen Informationen die Aktionen angezeigt, die Sie für das ausgewählte Bedienfeld durchführen können.

- 10 Suchfeld „PGP Keys“.** Hier können Sie nach Schlüssel in Ihrem Schlüsselbund suchen. Wenn Sie in diesem Feld Text eingeben, zeigt PGP Desktop Email 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 Desktop Email verwenden

PGP Desktop Email kann zur automatischen und transparenten Verschlüsselung und Signatur von ausgehenden Nachrichten und zur Entschlüsselung und Verifikation von eingehenden Nachrichten verwendet werden. Dazu versenden und empfangen Sie Ihre E-Mail ganz einfach wie gehabt; PGP Desktop Email übernimmt alles andere.

### Verschlüsselte E-Mail-Nachrichten senden

Nach der Installation wird PGP Desktop Email zwischen Ihrem E-Mail-Client und Ihrem Mail-Server eingefügt, wo er Ihren E-Mail-Verkehr überwacht.

Beim Eingang von *eingehenden* Nachrichten werden diese von PGP Desktop Email abgefangen, bevor sie in den Posteingang gelangen, und es wird automatisch versucht, sie zu entschlüsseln und zu verifizieren; zur Entschlüsselung werden Ihre privaten Schlüssel und zur Verifikation werden Ihre öffentlichen Schlüssel verwendet. Nach Abschluss dieser Maßnahmen werden Ihre Nachrichten von PGP Desktop Email in Ihren Posteingang zugestellt.

In den meisten Fällen brauchen Sie nichts weiter zu tun; entschlüsselte eingehende Nachrichten erscheinen in Ihrem Posteingang wie alle anderen eingehenden Nachrichten.

Beim Versenden von *ausgehenden* Nachrichten werden diese auf dem Weg zu Ihrem Mail-Server von PGP Desktop Email abgefangen und es wird automatisch versucht, sie auf der Grundlage der konfigurierten Grundsätze zu verschlüsseln und zu signieren.

Auch hier brauchen Sie nichts weiter zu tun; Sie erstellen einfach Ihre Nachrichten mit Ihrem E-Mail-Client und versenden sie — PGP Desktop Email übernimmt alles weitere.

Die nachfolgenden Abschnitte enthalten detaillierte Informationen zur transparenten Handhabung Ihrer eingehenden und ausgehenden Nachrichten durch PGP Desktop Email.

## Eingehende Nachrichten

PGP Desktop Email handhabt eingehende Nachrichten nach inhaltlichen Gesichtspunkten:

- **Weder verschlüsselt noch signiert.** Wenn eine Nachricht weder verschlüsselt noch signiert ist, wird sie von PGP Desktop Email einfach an Ihren E-Mail-Client weitergeleitet. Die Nachricht ist in ihrer jetzigen Form lesbar, so dass PGP Desktop Email nichts weiter tun muss.
- **Verschlüsselt, jedoch nicht signiert.** Wenn eine Nachricht verschlüsselt ist, versucht PGP Desktop Email, sie zu entschlüsseln, so dass sie gelesen werden kann. Zuerst wird Ihr Schlüsselbund nach dem privaten Schlüssel, der die Nachricht entschlüsseln kann, abgesucht. Wird der private Schlüssel gefunden, entschlüsselt PGP Desktop Email damit die Nachricht und leitet sie dann an Ihren E-Mail-Client weiter. Wenn der private Schlüssel nicht gefunden wird, leitet PGP Desktop Email die Nachricht verschlüsselt an Ihren E-Mail-Client weiter. Das sieht dann ungefähr so aus.

```
-----BEGIN PGP MESSAGE-----
Version: PGP Desktop 9.10
```

```
qANQR1DBWuDMvPGQkz1HwBD/0f5F8QkTY+1NVzwQw4xQ/EPu0D0mLrMzVvNQVn
rYVHPoACn6C3zfpo996akjr1o0Bga62hklpkjq13QEGpBTqMP1F64TuxqHkPLNH
ISN+7ZEA7EYtTV+3ErRE0H6yQgJ+sQGm6sJRjddyVTG6hGa9F2Wx+ZDLAIK6SrA
f4ZNQfNvkowmJX578S27LEGE5d5Wm68kKB/Ff1vfyZ1w360ggauIXmom9F8294p
fNawAnhQ1Rif/1a/MuYs0wkTLPQpDBXhgzqVkaE85gsCrwqxMAGDEYfrsCAB1Ne
rMwJNTXsRYvpstmpNBZuvH01jkrXE4YEAPk48MOD1Yi54NJxywvury79oDoxD1Jh
o9yh9v5f071orplFcew8wmlX4qagds0vqdwQRrfwbwnbgsd1jD2cmijyOq+bcy
3hZknIEgbb7GTka01cj+y9uSaFDh491A9qLyHTWWLuHYV/j/wtBPFpZpjGyVACV
FqRDE08hyZxkc/FoQw1Imdo+nymZEQITTTDBCaESxm5V+jBwfn0xhUK/Evy1kAHm
n27x2m9Pdwzxr1qjgrxI8Lda7DTJWymA8o120C1QzqrqvAmqIKL4CpckyhPurwIg
nan80KN/USfZK+v19juxM1155oGyz0Dtl6KnlNGGpTLu6YLSU25B7i1bve330ukJ
zMLXgdlAKQFSITPMVEKqJPXQrMrL1EYr6hE7FcAYmUWxe8W60e7H20wEime2Y9V
eVocS5p9Iau7w987Ifbh1oDEb+QEWJmav55JbCaE12hxAylFrIdXBb1REeuQGjmj
FUCHf6GGtp9H1Njw92iR5q5intRoh2KmwTa5oGbdNNEAAQ3p8SI+6129FLPLGF
z7/wzmKnFngV40gILxyPCrV56Pbo30WAg3ehhQDZC9KekmXd6J7t/caDEMUSnHC1
qTBA5CHRb+8En5yrUrZ5YUqhnvPr/vvN6odPenX4mbrMSc1v4uxRYSv5ofGHJTOU
=8hvs
-----END PGP MESSAGE-----
```

- **Signiert, jedoch nicht verschlüsselt.** Wenn eine Nachricht signiert ist, versucht PGP Desktop Email, die Signatur zu überprüfen. Die folgenden Speicherorte werden in dieser Reihenfolge auf den entsprechenden öffentlichen Schlüssel hin abgesucht: Ihr Standardschlüssel, der Keyserver auf keys.domain, wobei Domain die Domain des Absenders der Nachricht ist, das PGP Global Directory (keyserver.pgp.com), alle anderen konfigurierten Keyserver. Wenn PGP Desktop Email den entsprechenden öffentlichen Schlüssel findet, versucht es, die Signatur zu überprüfen und dann die Nachricht an Ihren E-Mail-Client weiterzuleiten. Falls PGP Desktop den entsprechenden öffentlichen Schlüssel nicht findet, wird die Nachricht unverifiziert an Ihren E-Mail-Client übergeben.
- **Verschlüsselt und signiert.** Wenn eine Nachricht verschlüsselt und signiert ist, versucht PGP Desktop Email zuerst, den privaten Schlüssel zur Entschlüsselung der Nachricht und dann den öffentlichen Schlüssel zur Verifizierung der Nachricht zu finden.

## Ausgehende Nachrichten

PGP Desktop Email handhabt Ihre abgehenden E-Mail-Nachrichten auf der Grundlage von Richtlinien bzw. Anleitungssätzen, die zur Handhabung jeder Situation festgelegt werden können.

## Standardrichtlinien

PGP Desktop Email umfasst vier Standardrichtlinien:

- **Mailing-Listen-Administratorabfragen.** Administratorabfragen an Mailing-Listen sollen als Klartext gesendet werden; d.h. weder verschlüsselt noch signiert.
- **Mailing-Listen-Sendevorgänge.** Sendevorgänge werden an Mailing-Listen signiert (damit sie authentifiziert werden können), jedoch nicht verschlüsselt gesendet.
- **Verschlüsselung erzwingen: [PGP] Vertraulich.** Alle als vertraulich markierten Nachrichten in Ihrem E-Mail-Client, oder die den Text „[PGP]“ in der Betreffzeile enthalten, müssen an einen gültigen öffentlichen Schlüssel eines Empfängers verschlüsselt werden, damit sie gesendet werden können. Diese Richtlinie gibt Ihnen ein Verfahren zur einfachen Handhabung von Nachrichten, die verschlüsselt gesendet werden *müssen*; sonst werden sie nicht gesendet.
- **Opportunistische Verschlüsselung** Legt fest, dass alle Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, unverschlüsselt (als Klartext) gesendet werden. Wenn sich diese Richtlinie als letzte Richtlinie in der Liste befindet, wird gewährleistet, dass Ihre Nachrichten immer gesendet werden (außer wenn sie als vertraulich markiert werden) (wenn auch als Klartext), selbst wenn kein Schlüssel zur Verschlüsselung für den Empfänger gefunden wird.

## Neue Richtlinien erstellen

PGP Desktop Email bietet die Möglichkeit zusätzlich zu den vier Standardrichtlinien neue Richtlinien zu erstellen und zu verwenden. Sie können Richtlinien auf der Grundlage vieler verschiedener Kriterien erstellen.

Vollständige Informationen zur Erstellung und Implementierung von Messaging-Richtlinien finden Sie im *PGP Desktop Anwenderhandbuch*.

## Wurde meine Nachricht verschlüsselt?

Da PGP Desktop Email seine Arbeit automatisch und transparent vollzieht, kann es vorkommen, dass Sie sich fragen, ob Ihre Nachricht wirklich verschlüsselt versendet wurde. Das ist aller Wahrscheinlichkeit nach der Fall, aber es gibt auch Möglichkeiten, das sicherzustellen.

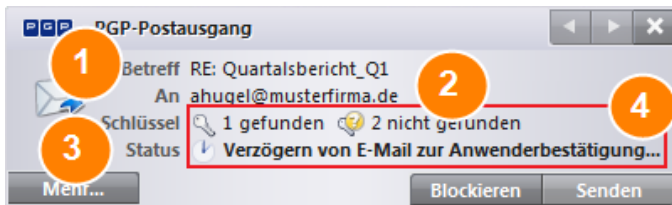
## Notifier-Warnungen

PGP Desktop Notifier-Warnungen sind eine Funktion von PGP Desktop, die Ihnen Einzelheiten zum Messaging mitteilt und Ihnen gleichzeitig Kontrolle darüber gibt.

Wenn Sie zum Beispiel eine verschlüsselte Nachricht versenden, erscheint in der rechten unteren Ecke des Bildschirms die Notifier-Warnung. Sie enthält folgende

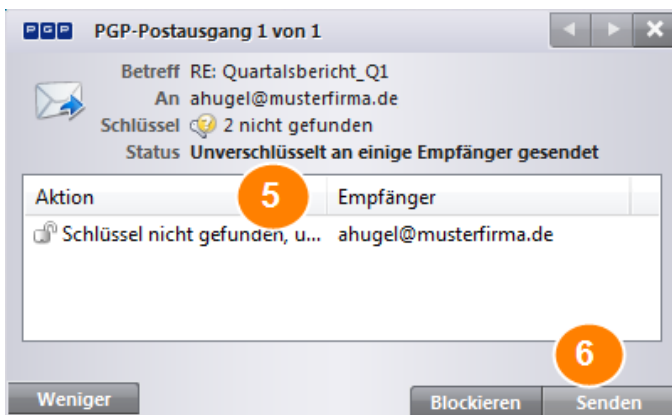
Einzelheiten:

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



Wenn Sie mehr Informationen über die versandte Nachricht sehen wollen, klicken Sie auf **Mehr**. Daraufhin werden auch folgende Informationen angezeigt:

5. Was PGP Desktop Email mit der Nachricht gemacht hat
6. Wer die Nachricht signiert hat



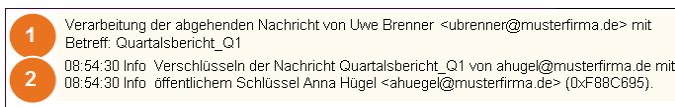
Nähere Informationen über Notifiers finden Sie im *Benutzerhandbuch für PGP Desktop*.

### PGP Log-Datei

Im PGP Log sind verschiedene Maßnahmen aufgelistet, die PGP Desktop Email zum Schutz Ihres Messaging ergreift.

Zum Beispiel hat die Nachricht, deren Notifiers oben aufgezeigt sind, diesen Eintrag in der PGP Log-Datei erzeugt. Sie enthält folgende Einzelheiten:

1. Dass eine abgehende Nachricht gesendet wurde, Absender und Betreff der Nachricht
2. Uhrzeit der Verschlüsselung; E-Mail-Adresse, an die die Verschlüsselung erfolgte; und die E-Mail-Adresse des Absenders



## PGP Virtual Disk-Laufwerke erstellen

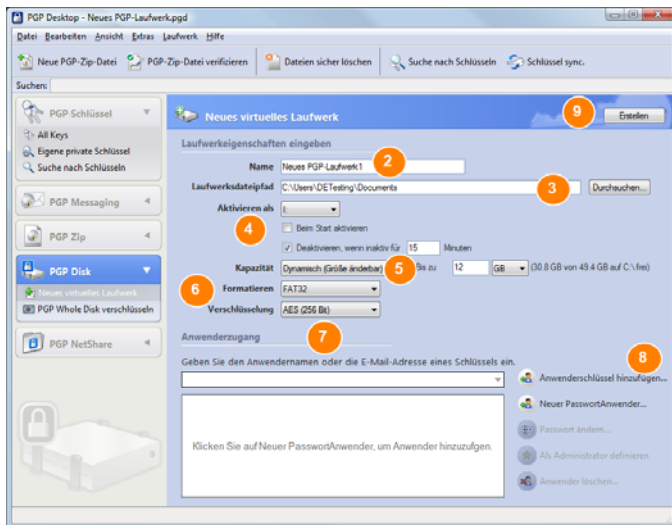
Die Funktion PGP Virtual Disk-Laufwerke verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit seinem eigenen Laufwerksbuchstaben. Sie können weitere Anwender für ein Laufwerk erstellen und dadurch autorisierten Personen den Zugriff gestatten.

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



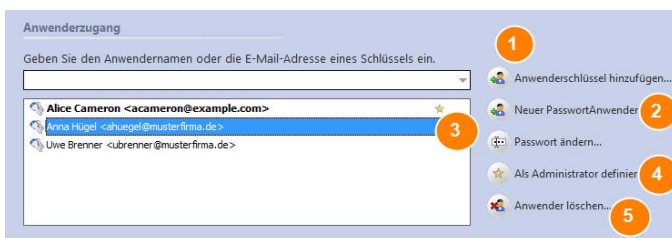
2. Geben Sie einen **Namen** für das Laufwerk ein.
3. Geben Sie einen **Laufwerksdateipfad** für das Laufwerk ein.
4. Geben Sie Ihre Aktivierungspräferenzen wie folgt an:
  - wählen Sie unter **Aktivieren als** einen Laufwerksbuchstaben für das Laufwerk aus.
  - wählen Sie **Beim Start aktivieren**, 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** den 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 Anwender 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) verwenden.

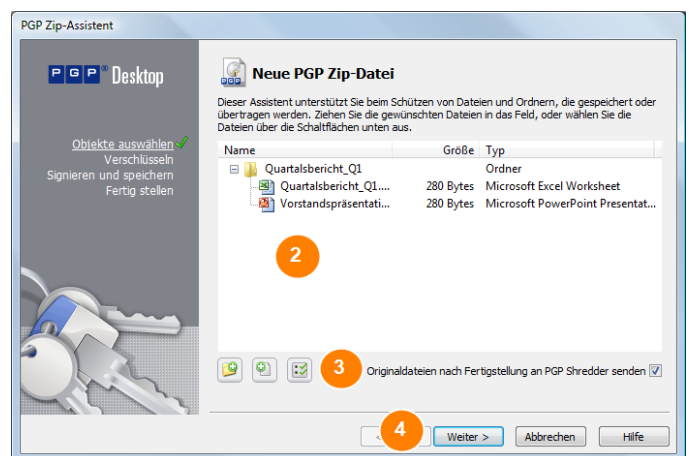
- **Passwort.** Verschlüsselt das Archiv für ein Passwort, das den Empfängern mitgeteilt werden muss. Die Empfänger müssen PGP-Software (für Windows oder Mac OS X) verwenden.
- **Selbstentschlüsselndes PGP-Archiv.** Verschlüsselt das Archiv für ein Passwort. Empfänger brauchen jedoch keine PGP-Software zu verwenden, um es zu öffnen, aber auf ihrem Computer muß Windows oder Mac OS X ausgeführt werden. 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-Software (für Windows oder Mac OS X) benutzen, um das Archiv öffnen und verifizieren zu können.

Die PGP Zip-Typen „Passwort“ und „Nur signieren“ sind im *PGP Desktop Anwenderhandbuch* näher 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**.

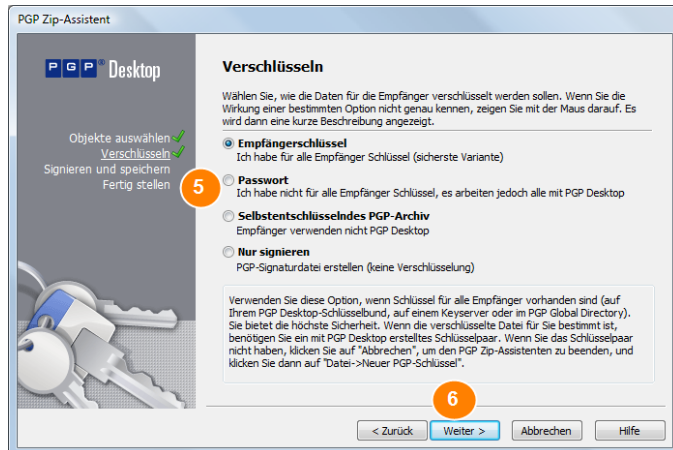


5. Wählen Sie den gewünschten Typ des PGP Zip-Archivs:

- **Empfängerschlüssel**
- **Passwort**
- **Selbstentschlüsselndes PGP-Archiv**

- **Nur signieren**

6. Klicken Sie auf **Weiter**.



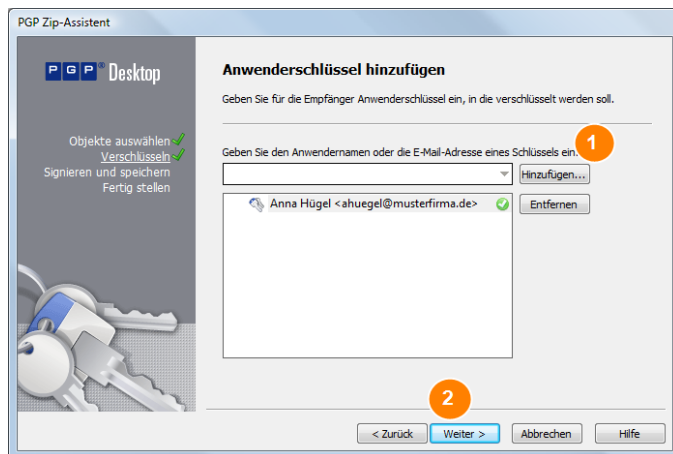
Die Typen **Passwort** und **Nur signieren** sind im *PGP Desktop Anwenderhandbuch* näher beschrieben.

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

## Empfängerschlüssel

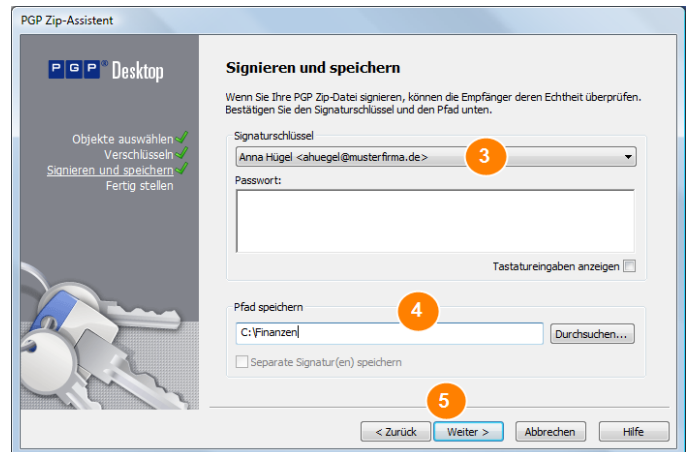
Der Bildschirm „Anwenderschlüssel hinzufügen“ erscheint.

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**.

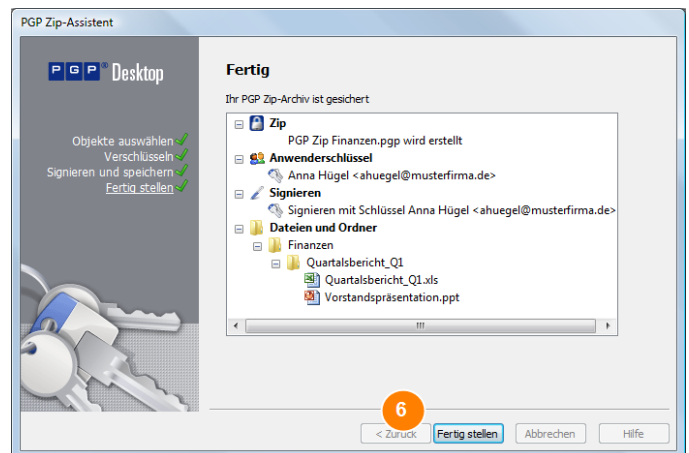


3. Wählen Sie einen privaten Schlüssel auf dem lokalen System, den Sie zur Signatur des Archivs verwenden.
4. Geben Sie einen Namen und einen Speicherort für das Archiv an. Der Standardname ist der Name der ersten Datei bzw. Ordners im Archiv; der Standardspeicherort ist der Speicherort der Dateien/Ordner,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

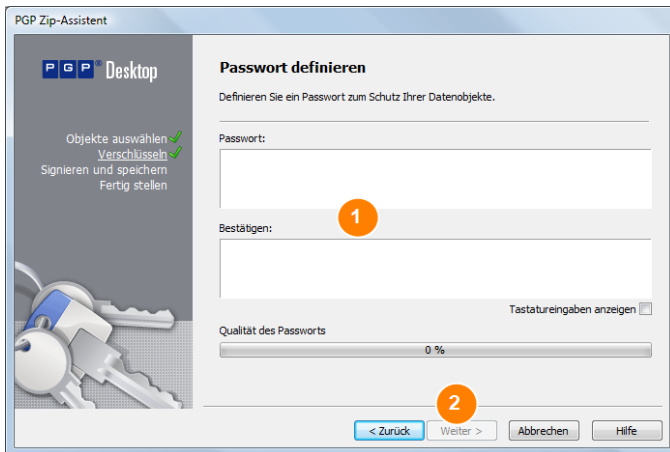
**Hinweis:** Der Typ „Nur signieren“ des PGP Zip-Archivs ist dem Typ Empfängerschlüssel sehr ähnlich; der einzige Unterschied ist, dass Sie keine öffentlichen Schlüssel auswählen, weil das Archiv lediglich signiert, jedoch nicht verschlüsselt wird.

## Selbstentschlüsselndes PGP-Archiv

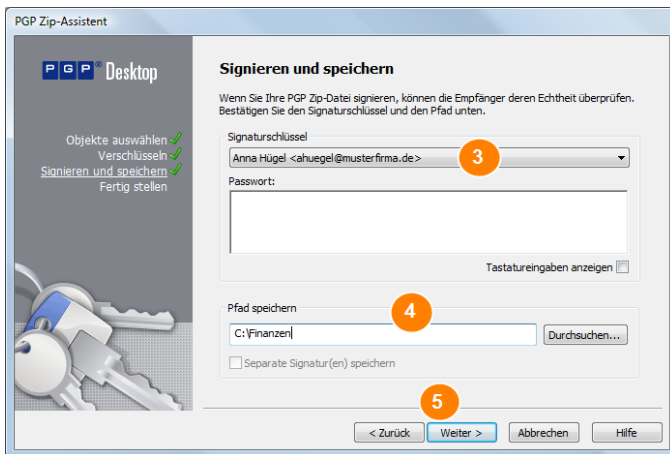
Der Bildschirm „Passwort definieren“ wird geöffnet.

1. Geben Sie ein Passwort für das PGP Zip Selbstentschlüsselnde Archiv (SDA) ein bestätigen Sie es, indem Sie es erneut eingeben.

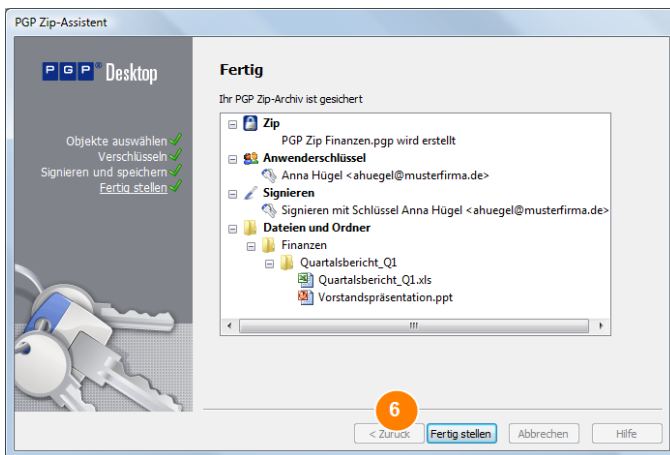
2. Klicken Sie auf **Weiter**.



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 Dateiwiederherstellungsoftware 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-Symbolleiste
- 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.

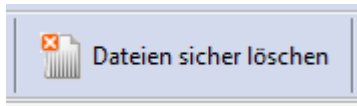


## Dateien mit der PGP-Symbolleiste sicher löschen

### ➤ So löschen Sie Dateien mit der PGP-Symbolleiste sicher

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

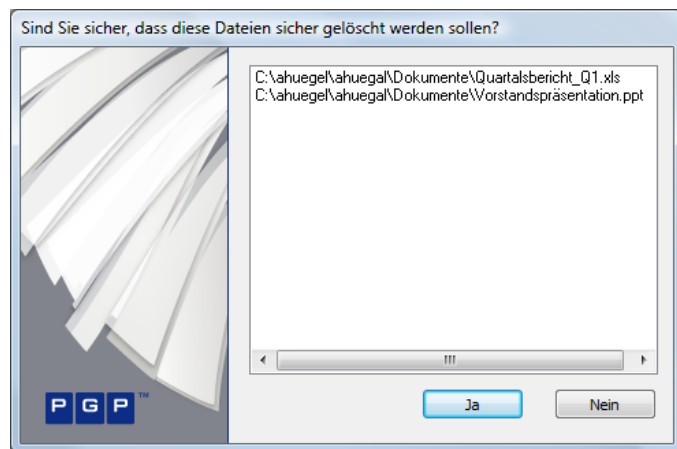
### ➤ So löschen Sie Dateien sicher in Windows Explorer

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 dazu **Extras > Optionen** aus, wählen Sie 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.

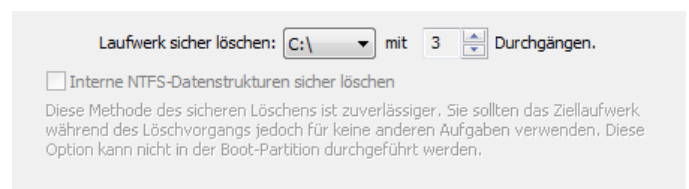
Wenn Sie Dateien in den Windows-Papierkorb ablegen und ihn leeren, werden die Dateien nicht wirklich gelöscht; Windows tut nur so, als ob sich dort nichts befindet und überschreibt die Dateien schließlich. Aber bis diese Dateien überschrieben werden, können sie leicht von einem Angreifer wiederhergestellt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

### ➤ So löschen Sie sicher freien Speicherplatz auf Ihren Laufwerken

1. Öffnen von PGP Desktop Email
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

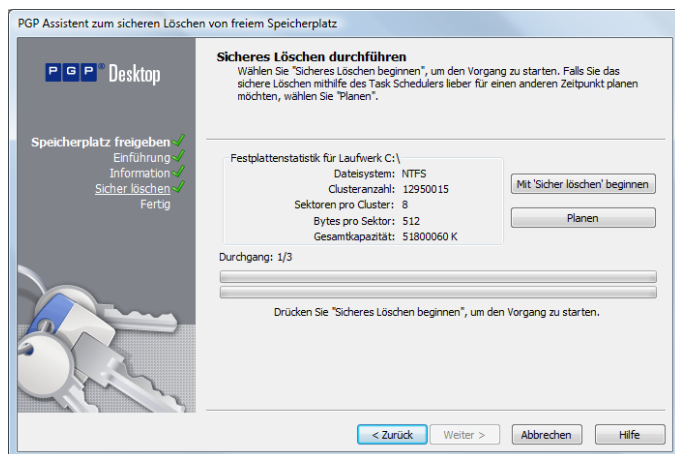


5. Wählen Sie ggf. die Option **Interne NTFS-Datenstrukturen sicher löschen** (nicht auf allen Systemen verfügbar) und klicken Sie dann auf **Weiter**. Diese Option löscht sicher kleine Dateien (unter 1KB) in internen Datenstrukturen, die anderenfalls nicht sicher gelöscht werden würden.
6. Klicken Sie 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 Löschens 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 die 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 Desktop Email-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 Desktop Email enthält auch eine integrierte Windows Online-Hilfe.

## 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.