

# Grundsätzliches zu Pretty Good Privacy

Mit dieser Anwendung kann man Emails o. Daten sicher übertragen, nur der berechnigte Empfänger kann sie lesen o. benutzen.

Schematische Vorgehensweise:

*Achtung! Falls PGP auf einem anderen System installiert ist oder war und schon ein Schlüsselpaar vorhanden ist (pubring.pkr secring.skr), bitte zuerst Seite 2 dieser Doku. "PGP Desktop-Installation von einem Computer auf einen anderen migrieren" lesen.*

*Bei Erstinstallation geht`s hier los:*

1. PGP Software installieren, Schlüsselpaar im Assistenten erzeugen lassen, Daten für Schlüsselerzeugung aufschreiben und sicher verwahren.  
(Achtung, bei Windows gleich richtiges Benutzerkonto auswählen)
2. Schlüssel zu Sicherungszwecken auf ext. Datenträger sichern (pubring.pkr secring.skr), Passwort aufschreiben o. merken!!! wenn Passwort weg, hat man verloren!
3. Öffentlichen Schlüssel (\*.asc o. \*.txt) per Email o. Datenträger dem „Kontaktpartner“ zukommen lassen, welcher mir sicher verschlüsselte Emails oder Dateien auf Datenträgern zusenden möchte.
4. Dieser „Kontaktpartner“ importiert zunächst meinen ihm zugestellten Schlüssel in seine PGP-Installation (einfach bei gestartetem PGP Schlüsseldatei per Doppelklick, PGP erkennt die Datei und nimmt den Schlüssel auf)
5. Um sicher zu stellen, dass der Absender authentisch ist, sollte der Schlüssel einmalig, vor erster Benutzung, verifiziert werden (Telefonisch, etc.). Den Fingerprint dazu kann man im PGP über Eigenschaften entnehmen.

Anwendung:

Mein „Kontaktpartner“ verschlüsselt Emails o. Datenfiles mit meinem, ihm vorher übertragenen, Schlüssel welchen er vorher in sein PGP importiert und mit mir verifiziert hat.

Man stelle sich vor er habe eine Kiste mit Vorhängeschloss von mir erhalten, packt die Daten in diese Kiste und drückt das Schloss zu. Nur wer den passenden Schlüssel besitzt kann die Kiste wieder öffnen und den Inhalt verwenden und das bin in diesem Fall nur ich.

# PGP Desktop-Installation von einem Computer auf einen anderen migrieren

Es ist nicht sehr kompliziert, eine PGP Desktop-Installation von einem Computer auf einen anderen zu verschieben („Migration“). Es müssen jedoch einige wichtige Schritte erfolgreich ausgeführt werden. Dieser Vorgang umfasst folgende Schritte:

So übertragen Sie eine PGP Desktop-Installation auf einen anderen Computer

1. Deinstallieren Sie PGP Desktop. Gehen Sie dazu auf **Start > Programme > PGP > PGP Desktop deinstallieren**. Sie können auch die Funktion „Software“ in der Systemsteuerung von Windows verwenden. Bei älteren Versionen des Programms ist die Entfernung über die Systemsteuerung die einzige Möglichkeit, PGP Desktop zu deinstallieren.

Beachten Sie, dass mit diesem Schritt die Schlüsselbunddateien nicht gelöscht werden.

2. Übertragen Sie die Schlüsselbunde. Kopieren Sie dazu die Schlüsselbunddateien (sowohl `pubring.pkr` als auch `secring.skr`) von dem alten Computer auf eine Diskette oder einen anderen Wechseldatenträger und dann auf den neuen Computer. Der Standardspeicherort für Schlüsselbunddateien ist `C:\Dokumente und Einstellungen\<Anwender>\Eigene Dateien\PGP\`.

Wenn PGP Desktop noch nie auf dem neuen Computer installiert war, müssen Sie diesen Ordner zuerst erstellen, bevor Sie die Schlüsselbunddateien auf den Computer kopieren.

3. Installieren Sie PGP Desktop auf dem neuen Computer. Laden Sie dazu PGP Desktop über den Download-Link in der ursprünglichen Bestellbestätigungs-E-Mail der PGP Corporation herunter.
4. Führen Sie dann während des Installationsvorgangs folgende Schritte aus:
  - Klicken Sie im Setup-Assistenten von PGP Desktop auf dem neuen Computer **Nein, ich habe bereits Schlüsselbunde** und geben Sie den Speicherort an, an dem Sie die Schlüsselbunddateien auf dem neuen Computer kopiert haben.
  - Verwenden Sie die gleichen Angaben für Name, Unternehmen und Lizenznummer, die bei der ursprünglichen Aktivierung von PGP Desktop verwendet wurden.