Was ist dieses „PGP"?

PGP steht für "Pretty Good Privacy". Es handelt sich dabei um ein Programm des US-Amerikaners Phil Zimmermann. Die erste Version fand bereits am 5. Juni 1991 ihren Weg in verschiedene Mailboxen.
PGP ermöglicht es, Nachrichten so zu verschlüsseln, dass nur der echte Empfänger sie lesen kann. Dabei kommen Verschlüsselungsalgorithmen zum Einsatz.

Und wie funktioniert PGP?

Herkömmliche Verfahren verwenden für das Codieren und Decodieren denselben Schlüssel. Der Empfänger kann die Nachricht nur lesen, wenn er den Schlüssel kennt, den der Absender verwendet hat. Dieses Verfahren hat einen großen Nachteil: Absender und Empfänger müssen sich auf einen gemeinsamen Schlüssel einigen und diesen austauschen. Dies geschieht naturgemäß unverschlüsselt, so dass die Möglichkeit besteht, dass schon diese Kommunikation überwacht wird. Ein Angreifer könnte dann alle weiteren Nachrichten mitlesen: Er hat ja bereits den Schlüssel.
Im Gegensatz zu diesem symetrischen Verfahren verwendet PGP eine asymetrische Verschlüsselung. Dabei besitzt jeder Kommunkationspartner zwei Schlüssel: Einen privaten und einen öffentlichen. Den öffentlichen Schlüssel kann man beliebig verteilen, per eMail, über eine Webseite oder auch auf Diskette. Mit diesem öffentlichen Schlüssel kann man Nachrichten nämlich nur verschlüsseln, nicht aber lesen. Und wenn ein Text auf diese Weise mit Hilfe des öffenlichen Schlüssels kodiert wurde, kann nur der Besitzer des passenden privaten Schlüssels den Text wieder entziffern.

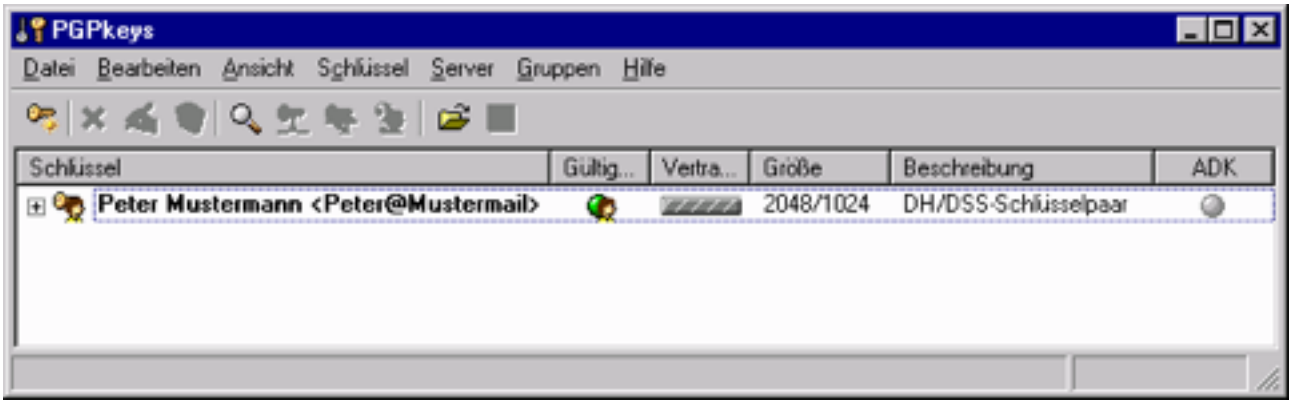
Wie nutze ich PGP?

Sie haben das Programm? Gut! Zuerst will PGP nun installiert werden. Das erfolgt wie bei anderen Windows-Programmen auch: Nach Angabe des Zielpfades wählen Sie die zu installlierenden Komponenten, den Rest übernimmt das Programm.
Bei der Komponentenauswahl sollte man Vorsicht walten lassen: PGP möchte standardmäßig seinen Treiber für Virtual Private Networks (VPNs) installieren. Wenn Sie nicht sicher wissen, dass Sie diesen nutzen wollen, deaktivieren Sie ihn. Sie ersparen sich damit eine Menge Arbeit.
PGP 8.0 bietet bei der Installation zwar Plugins und PGP-Disk Modul an, nutzbar sind diese in der Freeware-Version jedoch nicht. Eine Installation ist in diesem Fall überflüssig.
Am Ende der Installation bietet PGP Ihnen umgehend die Erzeugung eines neuen Schlüsselpaares an. Wählen Sie für den Anfang RSA mit 2048 Bit und denken Sie sich eine hübsche Passphrase aus. Tips dazu finden Sie hier.

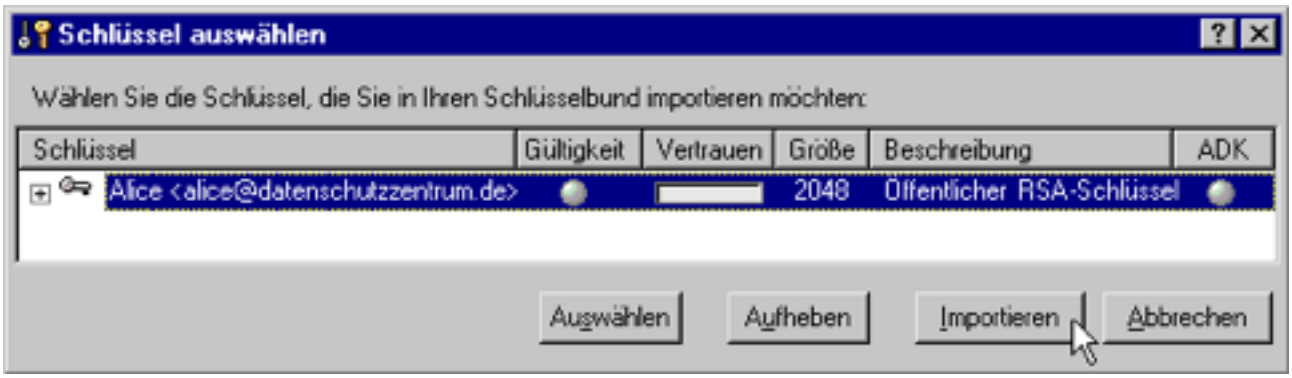
Wie bekomme ich PGP?

PGP können Sie hier laden.

Nach Abschluss der Schlüsselgenerierung sehen Sie ein Fenster wie dieses:



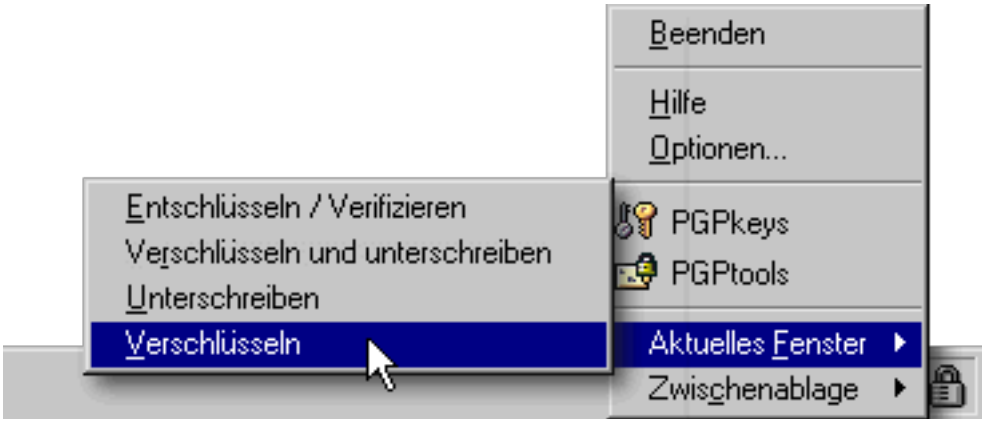
PGP-Keys ist die Schlüsselverwaltung von PGP. Hier können Sie sehen, mit wem Sie Schlüssel ausgetauscht haben, ob diese noch gültig sind und haben einen Überblick über Stärke und Typ der Schlüssel. Im Moment sieht das ganze noch etwas trostlos aus, Sie haben nur einen einzigen Schlüssel: Ihren eigenen.
Um mit einem Partner verschlüsselte eMails auszutauschen, benötigen Sie dessen öffentlichen Schlüssel. Den bekommen Sie entweder direkt von ihm (per eMail, von der Homepage oder auf Diskette) oder von einem Schlüsselserver. Dabei handelt es sich um Rechner im Internet, an die jeder seinen öffentlichen Schlüssel schicken kann. Von dort kann sich dann ein Kommunikationspartner den Schlüssel herunterladen, auch wenn der Besitzer gerade im Urlaub ist.
Für den Anfang können Sie sich den öffentlichen Schlüssel von Alice herunterladen und ihr eine Mail schreiben: Klicken Sie hier und kopieren Sie den Text in die Zwischenablage. Danach fügen Sie ihn in PGP-Keys ein: Klicken Sie einfach auf "Bearbeiten" und dann auf "Einfügen". PGP zeigt dann folgendes Meldungsfenster:



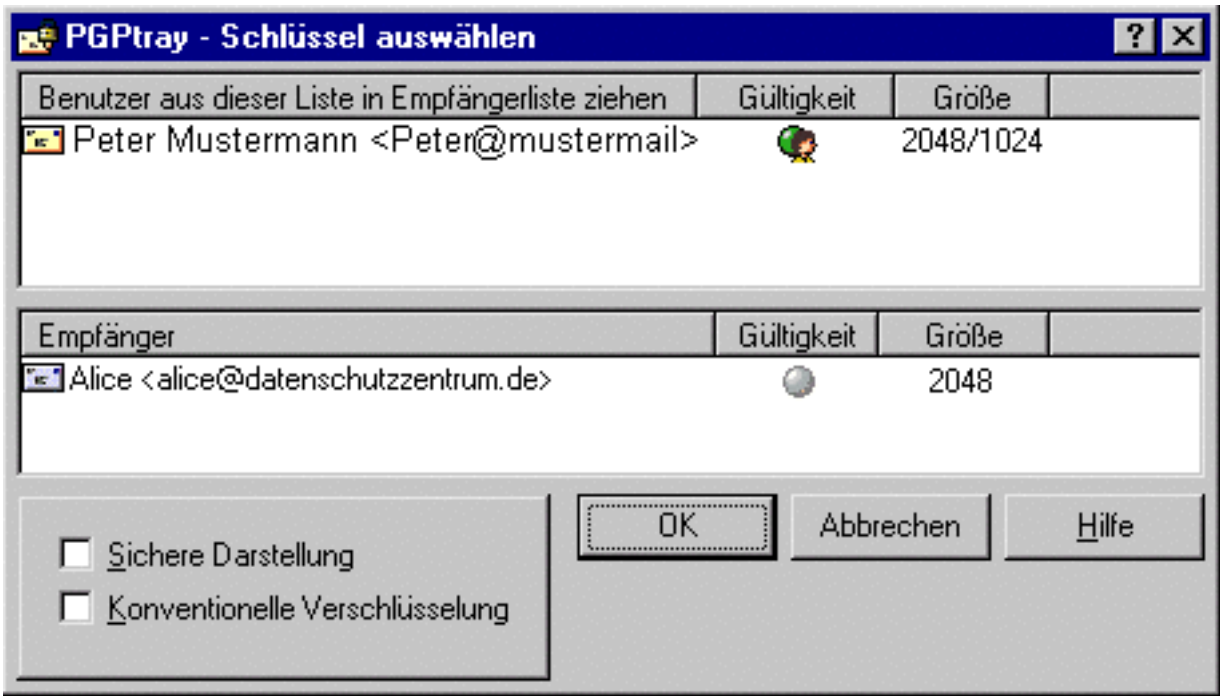
Mit einem Klick auf "Importieren" wird der Vorgang abgeschlossen. Sie haben nun den öffentlichen Schlüssel von Alice in ihren Schlüsselbund aufgenommen.

Die Vorbereitungen sind erledigt: Sie haben PGP installiert, einen eigenen Schlüssel erzeugt und einen weiteren importiert.

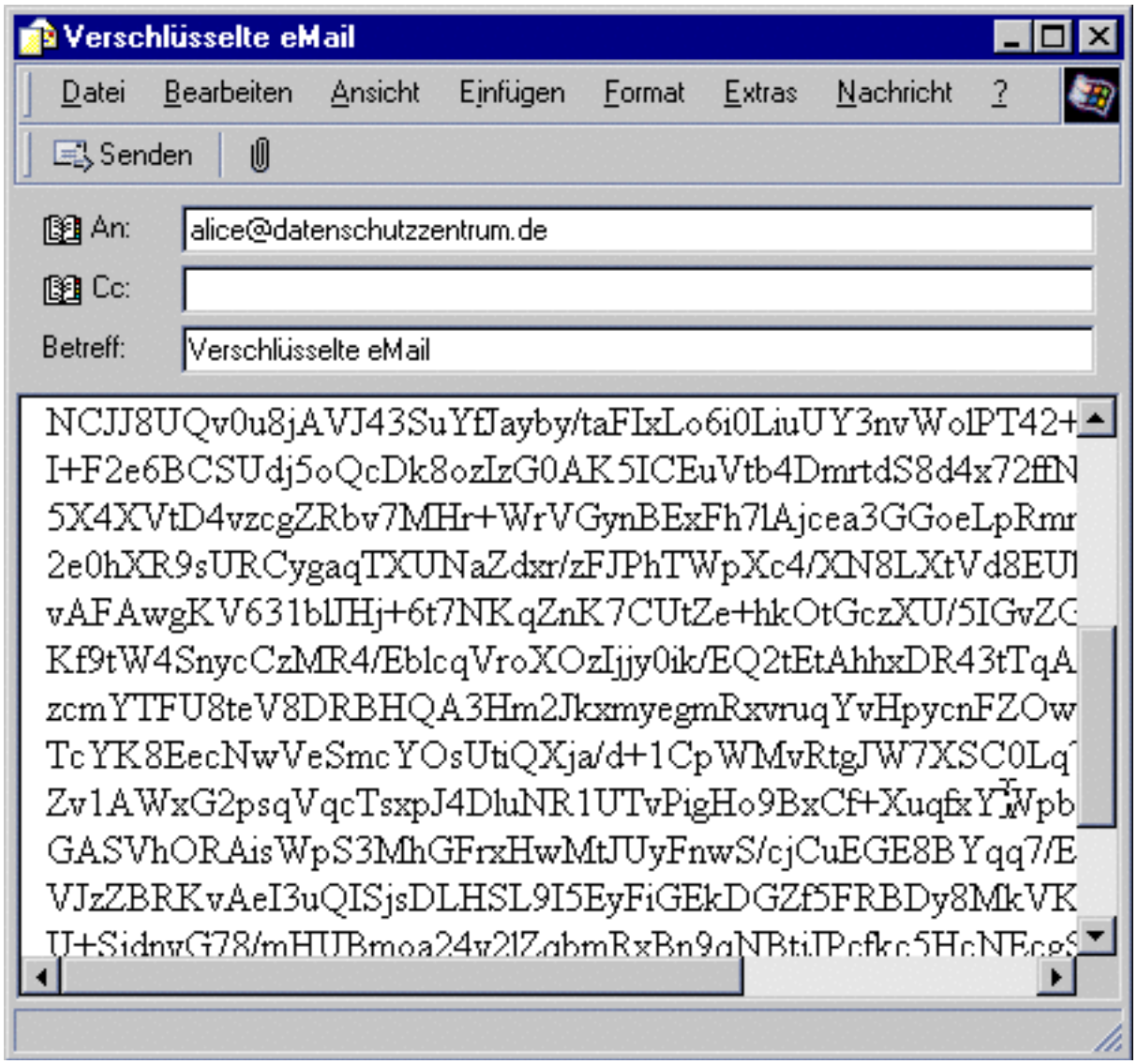
Um nun eine Mail zu verschlüsseln, öffnen Sie nun wie gewohnt Ihr eMail-Programm. Schreiben Sie ihre Mail und klicken Sie auf das kleine PGP-Tray Icon unten rechts in der Taskleiste:



Mit diesem Befehl können Texte in jeder Anwendung verschlüsseln. PGP ist also nicht von ihrem eMail-Programm abhängig. Egal, ob Sie Eudora, Pegasus, Netscape oder Outlook verwenden: Verschlüsseln können Sie immer!
Unter dem Menüeintrag 'Optionen' können Sie auch sogenannte Hotkeys einstellen. Das sind Tastenkombinationen, die bestimmte PGP Aktionen auslösen. Stellen Sie hier zum Beispiel [Alt]+[V] zum Verschlüsseln ein, brauchen Sie in Ihrem Mailprogramm nur noch diese Tastenkombination zu betätigen, damit die Nachricht verschlüsselt wird.
Als nächstes will PGP wissen, an wen der Text verschlüsselt werden soll. Dazu bietet es Ihnen die Einträge Ihres Schlüsselbundes an. Ziehen Sie den Eintrag von Alice in die Empfängerliste.
Achtung: Wenn Sie die Nachricht hinterher selbst noch lesen wollen, wählen Sie zusätzlich noch Ihren eigenen Schlüssel. So stellen Sie sicher, dass Sie selbst später noch Zugriff auf den Text haben.



Nach einem Klick auf OK wird die Nachricht verschlüsselt. Einen Augenblick später sieht die Mail dann so aus:



Ihre Mail kann so verschlüsselt an uns übersandt werden.. Dieser Text kann jetzt nur noch mit dem passenden Private-Key entziffert werden. So können Sie diese Nachricht versenden, ohne dass jemand ihren Inhalt erfährt.