

Öffentliche Schlüssel auf einem Keyserver bereitstellen

Verweise auf von PGP Universal verwaltete Umgebungen gelten nicht für die Produkte PGP Virtual Disk und PGP Virtual Disk Professional. Weitere Informationen zu verwalteten PGP Universal-Umgebungen finden Sie unter [„Zentral verwaltete“ versus „Einzelplatz-Anwender](#).

Die beste Methode, Ihren öffentlichen Schlüssel verfügbar zu machen, besteht darin, ihn auf einem öffentlichen Keyserver zu platzieren. Auf diese Weise können Ihnen andere Personen verschlüsselte E-Mails senden, ohne ausdrücklich eine Kopie Ihres Schlüssels anfordern zu müssen. Gleichzeitig müssen Sie und andere auch keine große Anzahl öffentlicher Schlüssel speichern, die Sie selten verwenden.

Weltweit gibt es zahlreiche Keyserver (darunter das PGP Global Directory), auf denen Sie Ihren Schlüssel allgemein zugänglich machen können. Falls Sie PGP Desktop in einer Domäne verwenden, die durch einen PGP Universal-Server geschützt ist, hat Ihr PGP-Administrator PGP Desktop mit entsprechenden Einstellungen vorkonfiguriert.

Wenn Sie mit einem Server für öffentliche Schlüssel arbeiten, sollten Sie Folgendes bedenken, bevor Sie Ihren Schlüssel senden:

- Ist dies tatsächlich der Schlüssel, den Sie verwenden möchten? Andere, die versuchen, mit Ihnen zu kommunizieren, könnten wichtige Information mit diesem Schlüssel verschlüsseln. Aus diesem Grund empfiehlt es sich, nur solche Schlüssel auf einem Keyserver zu platzieren, die tatsächlich von anderen verwendet werden sollen.
- Werden Sie sich an das Passwort für diesen Schlüssel erinnern? Sie benötigen das Passwort, um verschlüsselte Daten wiederherzustellen oder den Schlüssel zu widerrufen, falls Sie ihn nicht verwenden wollen.
- Anders als beim PGP Global Directory bleibt ein einmal hochgeladener Schlüssel auf dem Server. Einige öffentliche Keyserver lassen das Löschen von Schlüsseln nicht zu. Andere Server wiederum bieten Replizierungsfunktionen, die Schlüssel auch auf andere Keyserver kopieren. Das bedeutet, dass ein Schlüssel wieder auftauchen kann, nachdem Sie ihn von einem der Server gelöscht haben.

Die meisten Anwender legen ihre öffentlichen Schlüssel unmittelbar nach dem Erstellen ihres Schlüsselpaars im PGP Global Directory ab. Falls Sie Ihren Schlüssel schon im PGP Global Directory abgelegt haben, müssen Sie dies nicht wiederholen. In den meisten Fällen ist es nicht notwendig, den Schlüssel auf einen anderen Keyserver hochzuladen. Beachten Sie auch, dass andere Keyserver Schlüssel unter Umständen nicht verifizieren. Somit kann es bei Schlüsseln auf anderen Keyservern wesentlich aufwändiger sein, den Eigentümer des Schlüssels zum Vergleich des Fingerabdrucks zu kontaktieren.

So senden Sie Ihren öffentlichen Schlüssel manuell zu einem Keyserver:

1. Öffnen Sie PGP Desktop.
2. Achten Sie darauf, dass das Bedienfeld **PGP Keys** ausgewählt ist.
3. Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar, dessen öffentlichen Schlüssel Sie zum Keyserver senden möchten.
4. Klicken Sie auf **Senden an**. Wählen Sie in der Liste den Keyserver aus, an den Sie den öffentlichen Schlüssel senden wollen. Weitere Informationen finden Sie unter [Keyserver verwenden](#), wenn der Keyserver, den Sie an Ihren öffentlichen Schlüssel

senden möchten, nicht in der Liste vorhanden ist. PGP Desktop informiert Sie, wenn der öffentliche Schlüssel erfolgreich auf den Keyserver kopiert wurde.

Sobald Sie eine Kopie Ihres öffentlichen Schlüssels auf einem Keyserver platziert haben, ist er für andere Personen verfügbar, die Ihnen verschlüsselte Daten senden oder Ihre digitale Signatur überprüfen möchten. Auch wenn Sie andere Anwender nicht ausdrücklich auf Ihren öffentlichen Schlüssel hinweisen, können diese eine Kopie davon abrufen, indem sie den Keyserver nach Ihrem Namen oder Ihrer E-Mail-Adresse durchsuchen.

Viele Anwender geben die Webadresse für ihren öffentlichen Schlüssel am Ende ihrer E-Mail-Nachrichten an. In den meisten Fällen kann der Empfänger einfach auf die Adresse doppelklicken, um auf eine Kopie Ihres Schlüssels auf dem Server zuzugreifen. Einige Anwender drucken ihren PGP-Fingerabdruck sogar auf ihre Visitenkarte, um die Verifizierung zu erleichtern.

Dies ist eine Information von Alfons Lang EDV S&D