

## Öffentliche Schlüssel von einem Keyserver abrufen

Wenn der Empfänger der verschlüsselten E-Mail ein erfahrener PGP Desktop-Anwender ist, befindet sich wahrscheinlich eine Kopie seines öffentlichen Schlüssels auf dem PGP Global Directory-Server oder einem anderen öffentlichen Keyserver. Somit können Sie jederzeit eine Kopie seines aktuellen Schlüssels abrufen, wenn Sie eine E-Mail an diesen Empfänger senden möchten, und müssen auf Ihrem öffentlichen Schlüsselbund keine unüberschaubare Zahl von Schlüsseln speichern.

Es gibt eine Reihe von öffentlichen Keyserversn, wie etwa das von PGP gehostete PGP Global Directory, auf denen die Schlüssel der meisten PGP-Anwender zu finden sind. Wenn Ihnen der Empfänger keine Internet-Adresse mitgeteilt hat, unter der sein öffentlicher Schlüssel gespeichert ist, können Sie auf einen beliebigen Keyserver zugreifen und nach dem Namen oder der E-Mail-Adresse des Anwenders suchen. Die Suche führt nicht in jedem Fall zum Erfolg, denn nicht alle öffentlichen Keyserver werden regelmäßig mit dem Schlüsseldatenbestand der anderen Server synchronisiert.

Falls Sie in einer Domain arbeiten, die durch einen PGP Universal Server geschützt ist, kann der PGP-Administrator vorgeben, den Keyserver zu verwenden, der in den PGP Universal Server integriert ist. In diesem Fall ist PGP Desktop wahrscheinlich schon für den Zugriff auf den passenden PGP Universal-Server konfiguriert.

Analog dazu ist der PGP Universal-Server per Voreinstellung für die Kommunikation mit dem PGP Global Directory konfiguriert. Damit verteilt die PGP-Tasksteuerung die Prozesslast der Suche und Verifizierung von Schlüsseln.

So rufen Sie einen öffentlichen Schlüssel von einem Keyserver ab:

1. Öffnen Sie PGP Desktop und markieren Sie das Bedienfeld **PGP Keys**.
2. Wählen Sie im Bedienfeld **PGP-Schlüssel** die Option **Nach Schlüsseln suchen**. Im Arbeitsbereich wird das Dialogfeld „Nach Schlüsseln suchen“ angezeigt.
3. Legen Sie die Suchkriterien fest, und klicken Sie auf **Suchen**. Wenn Sie nur einen bestimmten Keyserver durchsuchen möchten, klicken Sie auf die Dropdown-Schaltfläche **Suchen** und wählen den Keyserver in der Liste aus. Wenn der Keyserver, auf dem Sie suchen möchten, derzeit nicht in der Liste ist, klicken Sie auf **Keyserver-Liste bearbeiten**, und fügen Sie ihn hinzu.

Bei der Suche nach Schlüsseln auf einem Keyserver lassen sich Werte für verschiedene Schlüsselmerkmale vorgeben. Für die meisten Operationen steht auch die Umkehrung zur Verfügung. So können Sie beispielsweise eine Suche mit dem Kriterium „Anwender-ID ist nicht Peter“ durchführen.

Die Ergebnisse des Suchlaufs werden angezeigt.

4. Wenn bei der Suche ein öffentlicher Schlüssel gefunden wurde, den Sie zu Ihrem Schlüsselbund hinzufügen möchten, klicken Sie im Bedienfeld PGP Keys auf **Zu eigenem Schlüsselbund hinzufügen**. Der ausgewählte Schlüssel wird zu Ihrem Schlüsselbund hinzugefügt.

Tipp: Wenn Sie die Suchkriterien so einstellen, dass nach einem sehr üblichen Namen (das Kriterium „Name“ enthält beispielsweise „Stefan“) gesucht wird, wird nur der erste Treffer

zurückgesendet. Das ist eine beabsichtigte Funktion, um das nicht autorisierte, massenhafte Abfragen von Schlüsseln (sogenanntes „Harvesting“) zum Zweck des Phishing zu verhindern. Wenn Sie häufig auftretende Namen oder Domänen verwenden, müssen Sie möglicherweise den vollständigen Namen oder die E-Mail-Adresse eingeben, um den korrekten Schlüssel zu finden.

Dies ist eine Information von Alfons Lang EDV S&D