# Workshop OpenPGP-Smartcard

Martin Gollowitzer
Free Software Foundation Europe

Chemnitzer Linuxtage, März 2010

## Abstract

Dieser Workshop soll den Besuchern die Einrichtung und Verwendung einer OpenPGP-Smartcard (wie etwa der Fellowship-Karte der FSFE) in Verbindung mit dem GNU Privacy Guard (GnuPG) anhand einer praktischen Vorführung näherbringen. Die Besucher des Workshops können im Rahmen des Workshops GnuPG und eine OpenPGP-Smartcard vollständig einrichten. Dabei auftretende Fragen können noch vor Ort beantwortet werden.

## Voraussetzungen

Der Workshop setzt keinerlei spezielles Wissen voraus. Da der Workshop auf Benutzer von GNU/Linux zugeschnitten ist, sollte dieses System schon einmal benützt worden sein. Es ist von Vorteil, wenn die Besucher bereits Erfahrung im Umgang mit der Shell haben. Falls es notwendig sein sollte, können aber auch diese Grundlagen kurz erklärt werden.

## Inhalt

Im ersten Teil wird die Einrichtung von GnuPG inklusive der Schlüsselgenerierung schrittweise durchgeführt. Dabei werden die einzelnen Befehle kurz erläutert und eventuell auftretende Probleme behandelt.

Nach der Generierung des Hauptschlüssels werden Unterschlüssel für die Verwendung mit der Smartcard generiert und auf diese übertragen. Dabei wird ein besonderes Augenmerk auf der Verhinderung von Datenverlust durch Sicherung der geheimen Schlüssel gelegt. Außerdem wird gezeigt, wie man eine OpenPGP-Smartcard personalisiert.

Nach der Einrichtung wird auf die tägliche Benutzung der Karte eingegangen. Es wird gezeigt, wie man Daten ver- und entschlüsselt, wie man mit Hilfe digitaler Signaturen die Integrität von aus dem Internet geladenen Daten überprüfen kann und wie man E-Mails digital signieren und/oder verschlüsselt verschicken kann. Aufgrund der großen Anzahl verfügbarer E-Mailbetrachter kann nur auf die am häufigsten verwandten eingegangen werden. In Absprache mit dem Auditorium werden dies aller Wahrscheinlichkeit nach Mozilla Thunderbird und/oder Evolution sein.

Der letzte Teil wird je nach verfügbarem zeitlichem Rahmen verschiedene weiterführende Themen, wie etwa das Signieren von Schlüsseln, der Aufbau eines Vertrauensnetzwerks (*„Web of Trust“*) oder auch sogenannte Keysigning-Partys behandelt. Wenn Interesse besteht, kann auch das Anmelden an Linux-Systemen mit PAM und die SSH-Authentifizierung mit der OpenPGP-Karte demonstriert werden.

Im Rahmen dieses Workshops soll auch das Nachdenken und die Diskussion über Themen wie Datensicherheit, Privatsphäre u.ä. angeregt werden.

## Literatur

Interessierte Besucher können sich bereits im Voraus über GnuPG und die Verwendung der OpenPGP-Smartcard informieren. Hilfreiche Informationsquellen sind unter anderem

- Die GnuPG-Dokumentation: http://gnupg.org/documentation/index.de.html
- Das OpenPGP card HowTo der FSFE:
  http://wiki.fsfe.org/Card_howtos/Card_with_subkeys_using_backups