

Organisation

KARLHEINZ GEYER

✉ streng@ftbfs.de

GPG-Schlüssel **0xaae6022e**

Fingerprint:

7A39 2F67 8CAE 262E 64FD

8A10 2F95 1508 AAE6 022E

MICHELE BORRELLI

✉ michele@borrelli.ch

GPG-Schlüssel **0x529b9e04**

Fingerprint:

7953 B830 5258 8154 4692

4DA1 B40F 6E26 529B 9E04

Quellen

[1] GNU-Handbuch der Privatsphäre

<http://www.gnupg.org/gph/de/manual>

[2] GNU-Privacy Guard

<http://www.gnupg.org>

[3] Hauptseite GZ Wipkingen

<http://www.gz-zh.ch>

[4] Teilnehmerliste aktuell

<http://zrh2k9-ksp.ftbfs.de/ksp-zrh2k9.txt>

[5] Relationsgraph aktuell

<http://zrh2k9-ksp.ftbfs.de/ksp-zrh2k9.svg>

[6] Hauptseite Keysigning-Party

<http://zrh2k9-ksp.ftbfs.de>

LINUX USER GROUP SWITZERLAND

KARLHEINZ GEYER MICHELE BORRELLI

Keysigning-Party Schweiz 2009

11. Dezember 2009 19.00 Uhr s. t.

Gemeinschaftszentrum Wipkingen
Breitensteinstrasse 19 a
CH- 8037 Zürich





Das Medium Internet ist aus unserer modernen Welt nicht mehr wegzudenken. Der Versand elek-

tronischer Daten spielt im Zeitalter der Compu- ter und der weitweiten Vernetzung eine herausragende Rolle. Privatpersonen, Firmen, Universitäten und Insti- tutionen nutzen diese preisgünstige Möglichkeit Daten und Nachrichten mittels E-Mail über das Internet zu ver- senden. So schnell und bequem das neue Medium als »Spediteur« für persönliche Daten, Forschungsergeb- nisse und Berichte auch sein mag, sicher ist es beiläube

Vom Sender zum Empfänger bewegen sich die Daten- pakete auf Wegen, die weder vorhersehbar noch frei wählbar sind. Datenpakete, welche schlecht oder gar un- verschlüsselt sind, können mitgelesen, verändert oder missbraucht werden. Der Austausch und die Benutzung von digitalen Schlüsseln sowie der Einsatz von krypto- grafischen Verfahren dienen massgeblich dem Schutz von **Vertraulichkeit, Integrität und Authentizität**. Wei- tere Informationen dazu sind im **Das GNU-Handbuch zum Schutz der Privatsphäre** [1] zu finden.

GNUPG

GNUPG [2] (GNU Privacy Guard) ist ein Programm zum Verschlüsseln und Signieren von digitalen Daten und arbeitet unabhängig von den jeweiligen Datenforma- ten (E-Mail, Textdateien, Bilddaten, Sourcecode, Daten- banken, komplette Festplatten usw.). Es entspricht der im RFC2440 festgelegten OpenPGP-Spezifikation und ist kompatibel zu PGP 5.x der Firma NA1. GNUPG ver- wendet dazu hauptsächlich ein hybrides Verfahren mit öffentlichem Schlüssel. Zum Verschlüsseln kann GNUPG aber ebenso auch ausschliesslich symmetrische Ver- fahren einsetzen und ist auf Linux/Unix, Mac OSx, MS- Windows ohne Einschränkungen lauffähig. Ferner ist GNUPG nicht - wie beispielsweise amerikanische Ver- schlüsselungsprogramme - aufgrund von Ausfuhrbestim- mungen im Umfang reduziert.

Keysigning-Party

Ziel einer solchen Veranstaltung ist es, einer möglichst grossen Anzahl von Personen die Möglichkeit zu eröffnen, ihre *Public-Keys* auszutauschen und sich ge- genseitig zu authentifizieren. Mit jeder Veranstaltung und dem daran angeschlossenen *Signieren der Schlüssel* wächst das so genannte *Netz des Vertrauens (Web-of-Trust)*.

Darüber hinaus lässt es sich bei einer Keysigning- Party vorzüglich über **Linux, Open-Source-Software, die Linux- und IT-Community**, Veranstaltungen, Mes- sen und Projekte diskutieren. So ergeben sich neue Kontakte und alte Freundschaften können gepflegt wer- den. Die kostenlosen Keysigning-Partys sind für alle in- teressant, denen **Computer- und Datensicherheit** ein ernstes Anliegen sind. Es ist sinnvoll, möglichst oft an Keysigning-Partys teilzunehmen; das verwendete Be- triebssystem spielt letztlich nur eine untergeordnete Rol- le.

Anmeldung zur KSP-ZRH2K9

Die nächste grosse Keysigning-Party findet am Freitag, 11. Dezember 2009 um 19.00 Uhr s. t. im **Gemein- schaftszentrum Wipkingen** statt. Zur Anmeldung genügt es, rechtzeitig bis **spätestens Dienstag, 8. Dezember 2009 23.59 Uhr** den eigenen GPG/PGP- Schlüssel auf dem dafür vorgesehenen Schlüsselserver abzuliegen. Verwenden Sie z. B. folgenden Befehl (in einer Zeile!):

```
gpg --keyserver hkps://zrh2k9-ksp.ftbfs.de --send-key KEY-ID
```

Spätestens am nächsten Tag sollten Sie Ihre Schlüsseldateien auf der Teilnehmerliste [4] und im Relationsgraphen [5] wiederfinden. Weitere Details zur geplanten Keysigning-Party entnehmen Sie bitte unserer Internetseite [6].

In Ausnahmefällen akzeptieren wir ihren öffentlichen GPG/PGP-Schlüssel auch als Anlage einer E-Mail, die Sie bitte mit der Betreffzeile **[KSP-ZRH2K9] Anmeldung** an strenge@ftbfs.de richten wollen. Zum Export Ihres Schlüssels verwenden Sie bitte folgenden Befehl:

```
gpg --armor --export KEY-ID > NameVorname.asc
```

Anreise

Ab Hauptbahnhof

Mit dem Tram 13 → Zürich, Albsgütli bzw. Tram 13 → Zürich, Frankental bis **Haltestelle Wipkingenplatz**, Fahrtzeit 13 Minuten ab/zum Bahnhof/Bahnstrasse.

Dankagung

Wir bedanken uns bei der **Linux User Group Switzer- land**(LUGS), denn ohne deren grossartiges Engagement wäre eine solche Veranstaltung sicher nicht möglich. Ein besonders herzliches Dankeschön geht an: AXEL BECKERT (XTaran) • MARTIN EBNÖTHER (Venty) • MA- RIUS RIEDER (Jiluka) • COSIMA JOERGENS (Jeanny) • MARTIN ZOBEL-HELAS (zobel) • ALEXANDER WIRT (for- more) • FABIAN ABPLANALP (fabiana) u. v. a. m. Danke für eure/ihre Unterstützung!