

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 der ETH Zürich
<http://www.ethz.ch/>

[4] Teilnehmerliste aktuell
<http://ethz08-ksp.ftbfs.de/ksp-ethz08.txt>

[5] Relationsgraph aktuell
<http://ethz08-ksp.ftbfs.de/ksp-ethz08.svg>

[6] Hauptseite der ETH-Keysigning-Party
<http://ethz08-ksp.ftbfs.de/>

LINUX USER GROUP SWITZERLAND

KARLHEINZ GEYER MICHELE BORRELLI

Keysigning-Party Schweiz 2008

12. Dezember 2008 19.00 Uhr s. t.

ETH Zürich
Campus Zentrum
Hauptgebäude (HG)
Erdgeschoss, Raum E 21
Rämistrasse 101
CH- 8092 Zürich



Mit freundlicher Unterstützung der

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

¹ Vorwort



Das Medium Internet ist aus unserer modernen Welt nicht mehr wegzudenken. Der Versand elektronischer Daten spielt im Zeitalter der Computer und der weltweiten Vernetzung eine herausragende Rolle. Privatpersonen, Firmen, Universitäten und Institutionen nutzen diese preisgünstige Möglichkeit Daten und Nachrichten mittels E-Mail über das Internet zu versenden. So schnell und bequem das neue Medium als «Spediteur» für persönliche Daten, Forschungsergebnisse und Berichte auch sein mag, sicher ist es beileibe nicht.

Vom Sender zum Empfänger bewegen sich die Datenpakete auf Wegen, die weder vorhersagbar noch frei wählbar sind. Datenpakete, welche schlecht oder gar unverschlüsselt sind, können mitgelesen, verändert oder missbraucht werden. Der Austausch und die Benutzung von digitalen Schlüsseln sowie der Einsatz von kryptografischen Verfahren dienen massgeblich dem Schutz von **Vertraulichkeit**, **Integrität** und **Authentizität**. Weitere 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 Datenformaten (E-Mail, Textdateien, Bilddaten, Sourcecode, Datenbanken, komplette Festplatten usw.). Es entspricht der im RFC2440 festgelegten OpenPGP-Spezifikation und ist kompatibel zu PGP 5.x der Firma NAI. GnuPG verwendet dazu hauptsächlich ein hybrides Verfahren mit öffentlichem Schlüssel. Zum Verschlüsseln kann GnuPG aber ebenso auch ausschliesslich symmetrische Verfahren einsetzen und ist auf Linux/Unix, Mac OS X, MS-Windows ohne Einschränkungen lauffähig. Ferner ist GnuPG nicht - wie beispielsweise amerikanische Verschlüsselungsprogramme - aufgrund von Ausführbestimmungen künstlich in seiner Funktionalität und Sicherheit

eingeschränkt.

Keysigning-Party

Ziel einer solchen Veranstaltung ist es, einer möglichst grossen Anzahl von Personen die Möglichkeit zu eröffnen, ihre *Public-Keys* auszutauschen und sich gegenseitig 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 vortrefflich über **Linux**, **Open-Source-Software**, die **Linux- und IT-Community**, Veranstaltungen, Messen und Projekte diskutieren. So ergeben sich neue Kontakte und alte Freundschaften können gepflegt werden. Die kostenlosen Keysigning-Partys sind für alle interessant, denen **Computer- und Datensicherheit** ein ernstes Anliegen sind. Es ist sinnvoll, möglichst oft an Keysigning-Partys teilzunehmen; das verwendete Betriebssystem spielt letztlich nur eine untergeordnete Rolle.

Anmeldung zur KSP-ETHZ08

Die nächste grosse Keysigning-Party findet am Freitag, 12. Dezember 2008 um 19.00 Uhr s. t. an der ETH [3] Zürich statt. Zur Anmeldung genügt es, rechtzeitig bis **spätestens Dienstag, 9. Dezember 2008 23.50 Uhr** den eigenen GPG/PGP-Schlüssel auf dem dafür vorgesehenen Schlüsselservers abzuliegen. Verwenden Sie z. B. folgenden Befehl (in einer Zeile!):

```
gpg --keyserver hkp://ethz08-ksp.ftbfs.de  
--send-key KEY-ID
```

Spätestens am nächsten Tag sollten Sie Ihre Schlüsseldaten 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-ETHZ08 Anmeldung* an streng@ftbfs.de richten wollen. Zum Export Ihres

Schlüssels verwenden Sie bitte folgenden Befehl:
`gpg --armor --export KEY-ID > NameVorname.asc`

Anreise

Ab Hauptbahnhof

In sechs Minuten mit dem Tram Nr. 6 → Zoo ab Hauptbahnhof (Bahnhofstrasse) oder mit dem Tram Nr. 10 → Bahnhof Oerlikon ab Hauptbahnhof (Bahnhofplatz) **Haltestelle Universitätsspital**, das ist die 3. Station nach dem Hauptbahnhof. Sie stehen nun direkt gegenüber dem Hauptgebäude der ETH Zürich. In der Eingangshalle rechts befindet sich die Info Loge.

In drei Minuten mit dem Tram Nr. 3 ab Hauptbahnhof (Bahnhofplatz) bis **Haltestelle Central** (1 Station) und ab Central mit der Polybahn, Abfahrt alle drei Minuten → **Polyterrasse**.

Ab Höggerberg

ETH-Pendelbus während des Semesters. Der ETH-Pendelbus fährt stündlich Montag–Freitag, benutzungsberechtigt sind Studierende mit gültiger ETH-Legi bzw. UNI-Legi sowie Mitarbeitende der ETH mit Identitätskarte.

Danksagung

Wir bedanken uns bei der **Linux User Group Switzerland** (LUGS) und der ETH Zürich für deren grossartiges Engagement, ohne das eine solche Veranstaltung nicht möglich wäre. Ein besonders herzliches Dankeschön geht an: AXEL BECKERT (XTaran) • MARTIN EBNÖTHER (Venty) • MARIUS RIEDER (Jiuka) • PRISKA RUBISCHON (Codo) • MARTIN ZOBEL-HELAS (zobel) • ALEXANDER WIRT (formorer) • DR. MATTEO CORTI u. v. a. m. Danke für eure/Ihre Unterstützung!

¹ © 11.2008 Karlheinz Geyer und Michele Borrelli