

## Organizzazione

KARLHEINZ GEYER

✉ [streng@ftbfs.de](mailto:streng@ftbfs.de)

Codice GPG **0xaae6022e**

Fingerprint:

7A39 2F67 8CAE 262E 64FD

8A10 2F95 1508 AAE6 022E

MICHELE BORRELLI

✉ [michele@borrelli.ch](mailto:michele@borrelli.ch)

Codice GPG **0x529b9e04**

Fingerprint:

7953 B830 5258 8154 4692

4DA1 B40F 6E26 529B 9E04

## Fonti

[1] Manuale GNU per la privacy

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

[2] GNU-Privacy Guard

<http://www.gnupg.org/>

[3] Pagina principale del PFS Zurigo

<http://www.ethz.ch/>

[4] Elenco aggiornato dei partecipanti

<http://ethz08-ksp.ftbfs.de/ksp-ethz08.txt>

[5] Raffigurazione aggiornata delle relazioni di fiducia

<http://ethz08-ksp.ftbfs.de/ksp-ethz08.svg>

[6] Pagina principale del Keysigning-Party del PFS

<http://ethz08-ksp.ftbfs.de/>

LINUX USER GROUP SWITZERLAND

KARLHEINZ GEYER MICHELE BORRELLI

# Keysigning-Party Svizzera 2008

12 dicembre 2008, ore 19.00

PFS di Zurigo  
Campus Centro  
Edificio principale  
Piano terreno, aula 21  
Rämistrasse 101  
CH- 8092 Zurigo



Con la gentile collaborazione del  
PFS Politecnico Federale Svizzero

**ETH**

Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich



Lo strumento Internet è diventato indispensabile per il nostro mondo moderno. L'invio di dati elettronici ha assunto un ruolo molto importante nell'era del computer e del collegamento in rete a livello mondiale. Persone private, ditte, università ed istituzioni ricorrono a questa opportunità economica per inviare dati ed informazioni tramite le e-mail via Internet. Il nuovo strumento può anche essere rapido e comodo per spedire dati personali, risultati di ricerche e relazioni, ma non è certamente un mezzo sicuro.

Dal mittente al destinatario, i pacchetti di dati si muovono su percorsi che non si possono né prevedere, né scegliere liberamente. I pacchetti di dati che sono crittografati male o non lo sono affatto, possono essere letti, modificati od usati a sproposito da altri. Lo scambio e l'uso di codici digitali, ma anche l'impiego di procedimenti crittografici servono in modo decisivo alla protezione della **riservatezza, integrità e autenticità**. Altre informazioni in proposito sono disponibili nel **manuale GNU per la protezione della privacy** [1].

## GNUPG

GNUPG [2] (GNU Privacy Guard) è un programma per la codifica e la firma di dati digitali e funziona indipendentemente dai relativi formati dei dati (e-mail, file di testo, dati di immagini, codice sorgente, banche dati, hard disk completi, ecc.). Esso è conforme alla specifica OpenPGP definita nell'RFC2440 ed è compatibile con GPG 5.x della ditta NAJ. GNUPG utilizza principalmente un procedimento ibrido con codice pubblico. Per la codifica, GNUPG può tuttavia usare anche procedimenti esclusivamente simmetrici ed è in grado di girare senza limitazioni su Linux/Unix, Mac OS X, MS-Windows. Inoltre, GNUPG non è limitato artificialmente nella sua funzionalità e sicurezza da normative sulle esportazioni - come avviene ad esempio per i programmi crittografici americani.

<sup>1</sup> © 11.2008 Karlheinz Geyer e Michele Borrelli

## Keysigning-Party

Lo scopo di tali manifestazioni è quello di offrire la possibilità al maggior numero di persone di scambiare le loro *Public Key* e di autenticarsi reciprocamente. Ad ogni manifestazione, con le conseguenti sottoscrizioni dei codici cresce la cosiddetta Rete di fiducia (Web-of-trust).

Inoltre, ad un Keysigning-Party è possibile discutere in modo proficuo su **Linux, Open Source software**, sulla **Linux e IT community** e su manifestazioni, fiere e progetti. In questo modo si creano nuovi contatti e possono essere ravvivate vecchie amicizie. I Keysigning-Party gratuiti sono di interesse per tutti coloro che considerano una questione seria la **sicurezza dei computer e dei dati**. È certamente utile partecipare al maggior numero possibile di Keysigning-Party; il sistema operativo usato ha soltanto un ruolo secondario.

### Iscrizione al KSP-ETHZ08

Il prossimo grande Keysigning-Party si terrà venerdì, 12 dicembre 2008 alle ore 19 in punto al PFS [3] di Zurigo. Per l'iscrizione è sufficiente registrare **entro martedì, 9 dicembre 2008, ore 23.50**, il proprio codice GPG/PGP sul server dei codici previsto per tale scopo. Utilizzate ad es. il seguente comando (su una sola riga!):

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

Al più tardi il giorno successivo dovrete trovare i vostri dati relativi al codice nella lista dei partecipanti [4] e nella raffigurazione delle relazioni di fiducia [5]. Ulteriori dettagli sul Keysigning-Party previsto sono presenti nel nostro sito Internet [6].

In casi particolari accettiamo il vostro codice GPG/PGP pubblico anche come allegato di un'e-mail, che invierete a `strenge@ftbfs.de` indicando in oggetto *KSP-ETHZ08 iscrizione*. Per l'esportazione del vostro codice, utilizzate il seguente comando:

```
gpg --armor --export KEY-ID < NomeCognome.asc
```

## Come raggiungereci

### Dalla stazione centrale

Sei minuti con il tram n. 6 → Zoo dalla **stazione centrale** (Bahnhofstrasse) o con il tram n. 10 → stazione Oerlikon dalla stazione centrale (Bahnhofplatz) **fermata Universitätsspital** (si tratta della terza fermata dopo la stazione centrale). Vi troverete così direttamente davanti all'edificio principale del PFS di Zurigo. Nella hall di ingresso a destra si trova il punto informativo.

### Polyterrasse.

Tre minuti con il tram n. 3 dalla stazione centrale (Bahnhofplatz) fino alla **fermata Central** (1 fermata) e da Central con la Polybahn, partenze ogni tre minuti → Servizio navetta PFS durante il semestre accademico. La navetta PFS parte ogni ora dal lunedì al venerdì; sono autorizzati ad usarlo gli studenti con Legi PFS o Legi UNI e i collaboratori del PFS con carta d'identità.

## Ringraziamenti

Desideriamo ringraziare il **Linux User Group Switzerland** (LUGS) e il PFS di Zurigo per il loro grande impegno, senza il quale non sarebbe stata possibile questa manifestazione. Un grazie di cuore va a: AXEL BECKERT (XTaran) • MARTIN EBNÖTHER (Venty) • MARIUS RIEDER (Juka) • PRISKA RUBISCHON (Codo) • MARTIN ZOBEL-HELAS (zobel) • ALEXANDER WIRT (formorer) DR. MATTEO CORTI e molti altri ancora. Grazie per il vostro sostegno!