

Organizzazione

KARLHEINZ GEYER

✉ streng@ftbfs.de

Codice GPG **0xaae6022e**

Fingerprint:

7A39 2F67 8CAE 262E 64FD

8A10 2F95 1508 AAE6 022E

MICHELE BORRELLI

✉ 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 Centro comunale Wipkingen

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

[4] Elenco aggiornato dei partecipanti

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

[5] Raffigurazione aggiornata delle relazioni di fiducia

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

[6] Pagina principale del Keysigning-Party

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

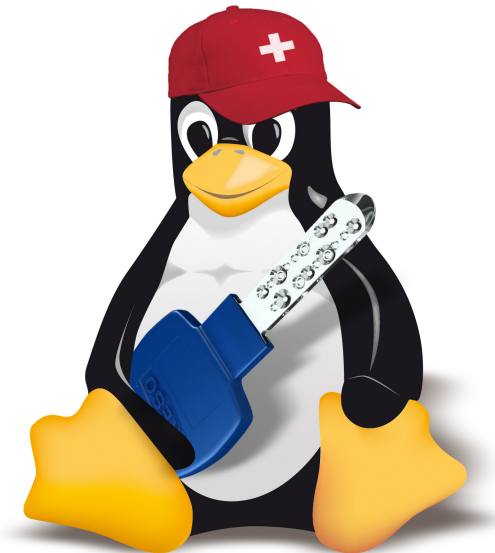
LINUX USER GROUP SWITZERLAND

KARLHEINZ GEYER MICHELE BORRELLI

Keysigning-Party Svizzera 2009

11 dicembre 2009, ore 19.00

Centro comunale di Wipkingen
Breitensteinstrasse 19 a
CH- 8037 Zurigo





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.

¹ © 11.2009 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-ZRH2K9

Il prossimo grande Keysigning-Party si terrà venerdì, 11 dicembre 2009 alle ore 19 in punto presso il Centro comunale di Wipkingen [3] in Zurigo. Per l'iscrizione è sufficiente registrare **entro martedì, 8 dicembre 2009, 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://zrh2k9-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-ZRH2K9/iscrizione]`. Per l'esportazione del vostro codice, utilizzate il seguente comando:

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

Come raggiungere

Dalla stazione centrale

Prendere il tram n. 13

reazione **Franckental** e scendere alla fermata **Wipkingerplatz**. Durata del tragitto: ca. 13 minuti.

Ringraziamenti

Desideriamo ringraziare il **Linux User Group Switzerland**(LUGS) per il suo grande impegno, senza il quale non sarebbe stata possibile questa manifestazione. Un grazie di cuore va a: AXEL BECKER (XTaran) • MARTIN EBNÖTHER (Venty) • MARIUS RIEDER (Juka) • COSIMA JOERGENS (Jeanmy) • MARTIN ZOBEL-HELAS (Zobel) • ALEXANDER WIRT (formorer) • FABIAN ABPLA-NALP (fabiana) e molti altri ancora. Grazie per il vostro sostegno!