

## Organisation

KARLHEINZ GEYER

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

Code GPG **0xaae6022e**

Fingerprint :

7A39 2F67 8CAE 262E 64FD

8A10 2F95 1508 AAE6 022E

MICHELE BORRELLI

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

Code GPG **0x529b9e04**

Fingerprint :

7953 B830 5258 8154 4692

4DA1 B40F 6E26 529B 9E04

## Sources

[1] Manuel GNU de la sphère privée

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

[2] GNU-Privacy Guard

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

[3] Page principale de l'EPF Zurich

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

[4] Liste actuelle des participants

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

[5] Graphique actuel des relations

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

[6] Page principale de l'EPF-Keysigning-Party

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

LINUX USER GROUP SWITZERLAND

KARLHEINZ GEYER MICHELE BORRELLI

# Keysigning-Party Suisse 2008

12 décembre 2008 19.00 heures

EPF Zurich  
Centre du campus  
Bâtiment principal  
Rez-de-chaussée, salle E 21  
Rämistrasse 101  
CH- 8092 Zurich



Avec l'amical soutien de  
l'EPF École polytechnique fédérale

**ETH**

Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich



Dans notre monde moderne, il est impossible de se passer du moyen de communication qu'est In-

ternet. Dans le siècle des ordinateurs et de l'in-terconnexion avec le monde entier, l'envoi de données électroniques joue un rôle prééminent. Particuliers, sociétés ; universités et institutions, tous utilisent cette possibilité avantagieuse en terme de coûts d'envoyer des données et des messages par e-mail par le biais d'Inter-net. C'est un « expéditeur » rapide et pratique de données personnelles, de résultats de recherche et de rapports mais qui n'est pas du tout sécurisé.

De l'expéditeur au destinataire, les paquets de données circulent par des chemins à la fois impossibles à prévoir et à choisir. Les paquets de données mal cryptés ou qui ne le sont pas du tout peuvent être lus, modifiées et utilisées abusivement. L'échange et l'utilisation de clés numériques ainsi que l'utilisation de procédés cryp-tographiques sont d'une importance déterminante en matière de protection de la **confidentialité**, de l'**intégrité** et de l'**authenticité**. Vous trouverez des informations complémentaires à ce sujet dans **Le manuel GNU sur la protection de la sphère privée** [1].

## GNUPG

GNUPG [2] (GNU Privacy Guard) est un logiciel de cryptage et de signature de données numériques qui fonctionne indépendamment des différents formats de données (e-mail, fichiers de texte, données en images, Sourcecode, banques de données, disques durs com-plets etc.). Il correspond à la spécification OpenPGP fixée dans RFC2440 et est compatible au PGP 5.x de la société NAJ. GNUPG utilise principalement un procédé hybride avec un code public. Pour crypter, GNUPG peut également n'utiliser que des procédés symétriques et peut fonctionner sans restriction sur Linux/Unix, Mac OSx, MS-Windows. Par ailleurs GNUPG n'est pas li-mité artificiellement en termes de fonctionnalité et de sécurité – comme par exemple les logiciels de cryptage

américains – par des dispositions en vigueur à l'exporta-

tion.

## Keysigning-Party

L'objectif d'une telle manifestation est d'ouvrir la possi-bilité au plus grand nombre de personnes d'échanger leurs *Public-Keys* et de s'authentifier réciproquement. A chaque manifestation et à la *signature des codes* qui lui succède, celui qu'on désigne comme le réseau de confiance devient plus grand (Web-of-Trust).

Par ailleurs, une Keysigning-Party est une excellente occasion de discuter de **Linux**, des **Open-Source-Software**, de la **Linux** et de l'**IT Community**, de manifestations, de salons et de projets. Elle per-met de nouer de nouveaux contacts et d'entretenir les anciennes amitiés. Les Keysigning-Partys gratuites sont intéressantes pour tous ceux qui se préoccupent sérieusement de la **sécurité des ordinateurs et des données**. Il est utile de participer le plus souvent pos-sible à des Keysigning-Partys, le système d'exploitation utilisé n'a qu'un rôle secondaire.

## Inscription à la KSP-ETHZ08

La prochaine grande Keysigning-Party se tiendra le vendredi 12 décembre 2008 à 19.00 heures à l'EPF [3] Zurich. Pour s'inscrire, il suffit d'enregistrer son code GPG/PGP sur le serveur de codes prévu à cet effet avant le **mardi 9 décembre 2008 à 23.50 heures au plus tard**. Vous pourrez par ex. utiliser la commande suivante (sur une ligne !):

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

Vous devriez retrouver vos données de code sur la liste des participants [4] et dans le graphique des relations [5] d'ici le lendemain au plus tard. Pour des informations complémentaires sur la Keysigning-Party programmée, veuillez consulter notre site Internet [6].

Dans des cas exceptionnels, nous acceptons de rece-voir votre code GPG/PGP public en annexe d'un e-mail que vous voudrez bien adresser à [strenge@ftbfs.de](mailto:strenge@ftbfs.de) en indiquant sur la ligne d'objet *Inscription KSP-ETHZ08*.

## Comment s'y rendre

### A partir de la gare centrale

En six minutes par le tram n° 6 → Zoo à partir de la **gare centrale** (Bahnhofstrasse) ou par le tram n° 10 → Gare Oerlikon à partir de la gare centrale (Bahnhofplatz) Arrêt **Universitätsspital**, c'est la 3<sup>ème</sup> station après la gare centrale. A votre arrivée, le bâtiment principal de l'EPF Zurich sera juste en face de vous. Dans le hall d'entrée à droite se trouve le local Info.

### A partir de Höggerberg

Bus pendulaire EPF pendant le semestre. Le bus pendu-laire circule toutes les heures du lundi au vendredi, sont autorisés à l'utiliser les étudiants en possession d'une Legi EPF ou d'une Legi UNI valide ainsi que les per-sonnes travaillant à l'EPF en possession de leur carte d'identité.

## Remerciements

Nous adressons nos remerciements au **Linux User Group Switzerland**(LUGS) et à l'EPF Zurich pour leur for-midable engagement sans lequel une telle manifestation n'aurait pas été possible. Un grand merci particulier à : AXEL BECKER (XTaran) • MARTIN EBNÖTHER (Venty) • MARIUS RIEDER (Jukka) • PRISKA RUBISCHON (Codo) • MARTIN ZOBEL-HELAS (zobel) • ALEXANDER WIRT (for-more) • DR. MATTEO CORTI Merci pour votre soutien !

suyvante :

Pour exporter votre code, veuillez utiliser la commande