Ma nouvelle clé PGP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 février 2014. Dernière mise à jour le 17 juin 2014

https://www.bortzmeyer.org/nouvelle-cle-pgp.html

Je viens de créer une nouvelle clé PGP, pour authentifier mes messages et pour qu'on puisse m'écrire de manière relativement confidentielle. En même temps, c'était l'occasion de créer une clé conforme aux bonnes pratiques de 2014, tenant compte de l'évolution de la cryptographie. C'est malheureusement plus dur que je ne le pensais.

Mon ancienne clé, portant le "*key ID*" 97D6D246 et l'empreinte BE25 EAD6 1B1D CFE9 B9C2 0CD1 4136 4797 97D6 D246 avait en effet été créée il y a treize ans ! Elle utilisait une clé DSA considérée comme trop courte aujourd'hui, vu les progrès de la cryptanalyse, ainsi que des algorithmes de cryptographie trop faibles. Depuis, les craqueurs ont eu tout le temps de trouver la clé privée... Voyons cette ancienne clé avec gpg :

```
% gpg --edit-key 97D6D246
Secret key is available.

pub  1024D/97D6D246  created: 2000-03-31  expires: never       usage: SC
                     trust: ultimate      validity: ultimate
sub  2048g/F08F74D7  created: 2000-03-31  expires: never       usage: E
[ultimate] (1). Stephane Bortzmeyer (Personal address) <stephane@bortzmeyer.org>
...

gpg> showpref
[ultimate] (1). Stephane Bortzmeyer (Personal address) <stephane@bortzmeyer.org>
     Cipher: AES256, AES192, AES, CAST5, 3DES
     Digest: SHA1, SHA256, RIPEMD160
     Compression: ZLIB, BZIP2, ZIP, Uncompressed
     Features: MDC, Keyserver no-modify
```