Clé PGP inutilisable ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 décembre 2021

https://www.bortzmeyer.org/pgp-key-half-expired.html

Décembre 2021, des correspondants m'informent que ma clé PGP n'est plus utilisable pour m'envoyer des messages chiffrés. "*Unusable public key*" ou autres messages peu parlants. Alors que ça marchait avant.

```
% gpg --encrypt --recipient CCC66677 toto.txt
gpg: CCC66677: skipped: Unusable public key
gpg: toto.txt: encryption failed: Unusable public key
```

C'était un simple oubli idiot de ma part : la clé a plusieurs sous-clés, ayant des rôles différents (chiffrement, signature…). Lors de la précédente expiration de la clé, j'avais bien re-signé mais en oubliant une des sous-clés, celle de chiffrement (une grosse bêtise). Au lieu d'un message clair du genre « cette clé a expiré » (ce qui se produit quand toutes les clés sont expirées), le logiciel, ne voyant que la clé de signature, n'arrivait pas à produire un message d'erreur intelligent. (Au passage, le format de clés PGP ou, plus exactement, OpenPGP, est normalisé dans le RFC 4880 [1]).

La clé et ses sous-clés, dont une (tout à la fin) était expirée :

```
sec  rsa4096/555F5B15CCC66677
     created: 2014-02-08  expires: 2023-12-21  usage: SC
     trust: unknown       validity: undefined
ssb  rsa4096/3FA836C996A4A254
     created: 2014-02-09  expires: 2023-12-21  usage: S
ssb* rsa4096/9045E02757F02AA1
     created: 2014-02-09  expired: 2021-12-19  usage: E
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4880.txt

("*Usage : E*" = "*encryption*" - chiffrement, alors que "*Usage : S*" désigne la possibilité de signer.)

Une fois tout re-signé proprement :

```
sec  rsa4096/555F5B15CCC66677
     created: 2014-02-08  expires: 2023-12-25  usage: SC
     trust: unknown       validity: undefined
ssb* rsa4096/3FA836C996A4A254
     created: 2014-02-09  expires: 2023-12-25  usage: S
ssb* rsa4096/9045E02757F02AA1
     created: 2014-02-09  expires: 2023-12-25  usage: E
```

Vous pouvez récupérer ma clé publique sur les serveurs de clés PGP habituels, ou bien directement sur ce site Web (en ligne sur `https://www.bortzmeyer.org/files/pgp-key.asc`). Les raisons pour lesquelles j'ai mis une date d'expiration à ma clé (ce n'est pas obligatoire et, vous avez vu, ça peut entrainer des problèmes), sont détaillées dans un autre article <`https://www.bortzmeyer.org/nouvelle-cle-pgp.html`>.

Merci à André Sintzoff pour le signalement et à Kim Minh Kaplan pour la solution.