Supprimer une clé SSH stockée par gpg-agent

Gpg-agent peut servir d’agent SSH (il va donc conserver les clés en mémoire) mais si l’ajout d’une clé se fait bien classiquement avec `ssh-add …`, la suppression d’une clé est plus complexe, `ssh-agent -d …` ne fonctionnant pas.

Repérer la somme MD5 de la clé à supprimer

Pour afficher les sommes MD5 des clés stockées par l’agent :

```
ssh-add -l -E md5
```

Ça donne un truc comme :

```
256 MD5:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa foo@bar (ED25519)
256 MD5:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb baz@qux (ED25519)
```

Si malheureusement vous n’avez pas spécifié le commentaire lors de la création de votre clé SSH, il y a des chances que vous vous retrouviez avec un truc comme :

```
256 MD5:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa foo@bar (ED25519)
256 MD5:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb foo@bar (ED25519)
```

Regardez bien la fin des lignes : vous ne savez pas quelle clé vous souhaitez supprimer !

Pour retrouver quelle somme MD5 correspond à quelle clé :

```
ssh-add -L
```

Ce qui affiche les clés publiques des clés SSH stockées, à savoir un truc comme :

```
ssh-ed25519 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX foo@bar
ssh-ed25519 YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY foo@bar
```

Un coup de `grep -RF XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX ~/.ssh` vous permettra d'identifier les clés. L'ordre entre `ssh-add -l -E md5` et `ssh-add -L` reste le même (heureusement).

Afficher le grip des clés stockées par gpg-agent

```
gpg-connect-agent 'KEYINFO --ssh-list --ssh-fpr' /bye
```

Ce qui donne un truc comme :

```
S KEYINFO VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV D - - - P
MD5:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa:aa - S
S KEYINFO ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ D - - - P
MD5:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb:bb - S
```

Le texte après le `KEYINFO` est le grip de la clé, qui va nous servir pour supprimer la clé :

```
gpg-connect-agent 'DELETE_KEY ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ' /bye
```

Et c'est fini

Révision #1
Créé 11 avril 2024 13:36:05 par Luc
Mis à jour 30 octobre 2024 12:09:38 par Luc