



Comment signer une clé GnuPG ?

Pour signer une clé GnuPG (aussi appelée GPG), il faut utiliser la commande dédiée afin de garantir l'authenticité d'une clé publique associée à une personne ou un tiers.^[1] ^[2]

Prérequis

- Disposer d'une paire de clés GPG installée sur votre machine (clé publique et clé privée).^[3]^[1]
- S'assurer d'avoir récupéré la clé publique à signer (souvent, elle a été importée dans votre trousseau de clés).^[2]

Étapes pour signer une clé GPG

1. Lister les clés présentes dans le trousseau :

```
gpg --list-keys
```

Relevez l'identifiant (ID) de la clé publique que vous souhaitez signer.^[1]

2. Éditer la clé à signer :

```
gpg --edit-key <ID-de-la-cle>
```

Remplacez <ID-de-la-cle> par l'identifiant de la clé cible.^[2]

3. Entrer la commande de signature dans le menu interactif :

```
sign
```

GPG va demander confirmation, puis votre mot de passe pour la signature. Après validation, la clé sera signée par votre identité GPG.^[2]

4. Envoyer la clé signée à son propriétaire (ou un serveur de clé) :

- Pour générer un fichier exportable :

```
gpg --export --armor <ID-de-la-cle> > cle-signee.asc
```

- Cette clé signée pourra ensuite être envoyée à la personne concernée ou publiée sur un serveur de clés.^[1]

Utilité de la signature

Signer une clé permet d'indiquer publiquement que vous avez vérifié l'identité de la personne à qui elle appartient, renforçant la confiance dans le réseau web of trust utilisé par GnuPG.^[1] ^[2]

Commande synthétique à retenir

```
gpg --edit-key <ID-de-la-clé>  
# puis dans l'interface : sign
```

N'oubliez pas de remplacer <ID-de-la-clé> par l'identifiant réel de la clé à signer.

Chaque étape doit être réalisée dans un terminal, la signature n'étant effective qu'après saisie de votre mot de passe secret et validation explicite.^[2] ^[1]

✱✱

1. <http://doc.ubuntu-fr.org/gnupg>
2. <https://www.gnupg.org/howtos/fr/GPGMiniHowto-3.html>
3. <https://www.sfeir.dev/securite/securite-signer-ses-commits/>
4. <https://serverspace.io/fr/support/help/creating-a-digital-signature-with-gpg/>
5. <https://docs.github.com/fr/authentication/managing-commit-signature-verification/generating-a-new-gpg-key>
6. <https://www.rvq.fr/linux/filecrypt.php>
7. <https://www.nbs-system.com/expertise/creation-de-sa-cle-gpg-et-utilisation-avec-passwordstore-eni-gmail-gpg-agent/>
8. <https://www.gnupg.org/howtos/fr/GPGMiniHowto-5.html>
9. https://www.youtube.com/watch?v=zXYyd3R_vPU
10. https://doc.fedora-fr.org/wiki/GnuPG_:._Signature_et_Chiffrement