

Gnu Privacy Guard (GnuPG) Mini Howto

lundi 30 juin 2014, par [placido](#)

Préambule

1. Quelques données sur les cryptosystèmes

1.1 Qu'est ce qu'un cryptosystème ?

1.2 Qu'est ce qu'un cryptosystème à clef publique ?

1.3 Qu'est ce qu'une signature numérique ?

1.4 Pourquoi signer une clef publique ?

1.5 Qu'est ce qu'un certificat de révocation ?

1.6 Est-il possible de lire mes messages chiffrés sans mon accord lorsque j'utilise GnuPG ?

2. Installation de GnuPG

2.1 Où récupérer les sources de GnuPG ?

2.2 Comment configurer la compilation de GnuPG ?

2.3 Comment compiler GnuPG ?

2.4 Comment installer GnuPG ?

3. Gestion de votre trousseau de clefs

3.1 Comment générer votre paire clef privée/clef publique ?

3.2 Comment rendre publique votre clef publique ?

3.3 Comment ajouter une clef publique à votre trousseau ?

3.4 Comment afficher le contenu de votre trousseau de clefs ?

3.5 Comment retirer des clefs de votre trousseau de clefs ?

3.6 Comment afficher l'empreinte d'une clef publique de votre trousseau de clefs ?

3.7 Comment signer une clef publique de votre trousseau de clefs ?

3.8 Comment générer un certificat de révocation pour une de vos paires de clefs ?

3.9 Comment modifier une clef publique de votre trousseau de clefs ?

4. Chiffrement et déchiffrement

4.1 Comment chiffrer un message ?

4.2 Comment déchiffrer un message ?

5. Signer et vérifier des signatures

5.1 Comment signer un message ?

5.2 Comment vérifier la signature d'un message ?

6. Documentations supplémentaires

6.1 GnuPG

6.2 PGP

6.3 Serveurs de clefs

6.4 Livres

7. Versions de ce document

Voir en ligne : [Gnu Privacy Guard \(GnuPG\) Mini Howto \(Français\)](#)