Tutoriel GPG pour Débutants

Cet aide-mémoire couvre les bases de l'utilisation de GPG (GNU Privacy Guard) pour chiffrer et signer des documents sur Linux, Windows et macOS.

Installation de GPG

Sous Linux

- Debian: `sudo apt install gnupg`
- Arch Linux: `sudo pacman -S gnupg`

Sous Windows

- Télécharger Gpg4win de Gpg4win.
- Exécuter le fichier d'installation et suivre les instructions à l'écran.

Sous macOS

- Installer GPG Suite de GPGTools.
- Ouvrir le fichier .dmg téléchargé et suivre les instructions d'installation.

Génération de la Clé GPG

- Ouvrir le terminal (Linux/macOS) ou Kleopatra (Windows).
- Exécuter `gpg –full-generate-key` (Linux/macOS) ou suivre l'assistant de création de clés (Windows).
- Choisir le type de clé et la taille.
- Entrer votre nom, adresse e-mail et commentaire.
- Définir un mot de passe fort pour la clé privée.

Sauvegarde de la Clé Privée

- Linux/macOS: `gpg –export-secret-keys [ID] > my-private-key.asc`
- Windows: Utiliser Kleopatra pour exporter la clé via l'interface graphique.

Création et Partage de la Clé Publique

- Linux/macOS: `gpg –armor –export [email]`
- Windows: Utiliser Kleopatra pour afficher et exporter la clé publique.

Chiffrement d'un Fichier

- Linux/macOS: `gpg –encrypt –recipient [email] fichier`
- Windows: Clic droit sur le fichier, “Chiffrer”, et sélectionner le destinataire.

Déchiffrement d'un Fichier

- Linux/macOS: `gpg –decrypt fichier.gpg > fichier`
- Windows: Clic droit sur le fichier chiffré, “Déchiffrer et vérifier”.

Signature de Fichiers

- Linux/macOS: `gpg –sign fichier`
- Windows: Clic droit sur le fichier, “Signer”.

Vérification des Signatures

- Linux/macOS: `gpg –verify fichier.sig fichier`
- Windows: Clic droit sur le fichier signé, “Déchiffrer et vérifier”.

Pour une meilleure compréhension et une gestion sécurisée, veillez à lire la documentation officielle de GPG et les guides de l’utilisateur de Gpg4win et GPGTools. La sécurité repose sur la bonne gestion des clés et des pratiques.