

Mission 2 : Authentification GPG

Explications

Définition

GnuPG est un outil open-source qui permet de chiffrer, décrypter, signer et vérifier

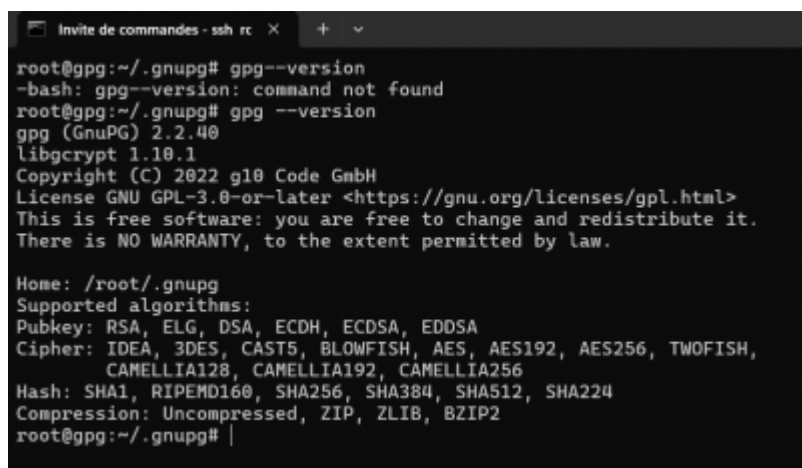
Installation de l'outil GPG

```
apt-get install gpg
```

Vérification

Après avoir installé GPG nous pouvons vérifier sa version en tapant la commande

```
gpg --version
```



```
root@gpg:~/.gnupg# gpg--version
-bash: gpg--version: command not found
root@gpg:~/.gnupg# gpg --version
gpg (GnuPG) 2.2.40
libgcrypt 1.10.1
Copyright (C) 2022 g10 Code GmbH
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /root/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
root@gpg:~/.gnupg#
```

Le dossier .gnupg

Le dossier .gnupg est essentiel pour GnuPG et stocke les clés de chiffrement et les fichiers de configuration. Voici son contenu typique :

- pubring.kbx : Contient les clés publiques, utilisées pour chiffrer des messages ou vérifier des signatures.
- private-keys-v1.d/ : Stocke les clés privées, nécessaires pour déchiffrer et signer des messages.
- trustdb.gpg : Gère les informations de confiance liées aux clés publiques.
- gpg.conf : Fichier de configuration pour personnaliser GnuPG.
- random_seed : Aide à générer des nombres aléatoires pour sécuriser les clés.

Certificats de révocation : Permettent d'invalider une clé si elle est compromise. En résumé, ce dossier assure la sécurité des clés, la configuration personnalisée et la gestion de la confiance dans GnuPG.

Configurations

From:

<https://sisr2.beaupeyrat.com/> - **Documentations SIO2 option SISR**

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-europe:chiffrement>

Last update: **2024/09/26 08:54**

