

## PGP :

PGPse propose de garantir la confidentialité et l'authentification pour la communication des données. Il est souvent utilisé pour la signature électronique de données, le chiffrement et le déchiffrement de textes, courriels, fichiers, répertoires et partitions de disque entier pour accroître la sécurité des communications. Utilisant la cryptographie asymétrique mais également la cryptographie symétrique, il fait partie des algorithmes de cryptographie hybride. PGP et les produits similaires suivent le standard OpenPGP (RFC 48803) pour le chiffrement et le déchiffrement de données.

### PG permet de :

Signer des messages ou fichiers. Chiffrer des messages ou fichiers. Déchiffrer des messages ou fichiers. Il propose aussi d'autres fonctions comme vérifier une signature, créer et gérer ses clés, et échanger des clés.

### Avantages :

Simplifie le partage des clés car les clés publiques sont accessibles à tous. Moins de clés à gérer dans un groupe. Inconvénients :

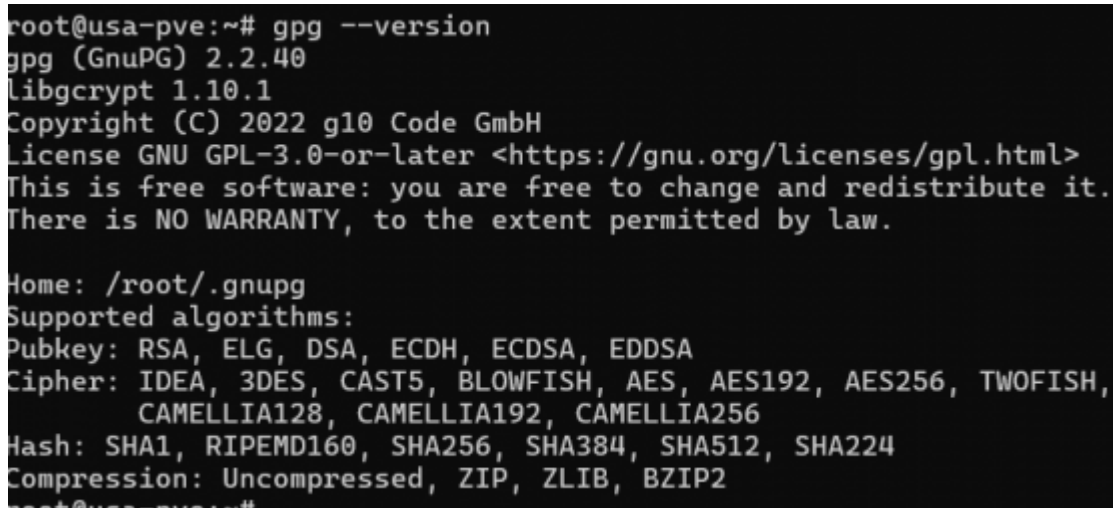
Plus lent que les méthodes de chiffrement symétrique. Pas de garantie que la clé publique est celle de la bonne personne. La sécurité repose entièrement sur la protection de la clé privée. Certains chiffrement symétriques peuvent être plus sûrs.

Quelques commandes importantes et des captures d'écrans réalisés au cours du test de PGP.

## Configuration de GPG

### installation de gpg et vérification de la version

```
gpg --version
```



```
root@usa-pve:~# 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@usa-pve:~#
```

Génération de la clé principale et vérification d'une eventuelle clé publique et privées sur ma machine :

## Génération de la clé principale

```
root@usa-pve:~# gpg --full-generate-key --expert
```

Créer une clé maître qui ne doit pouvoir que (C)ertifier

```
Please select what kind of key you want:
(1) RSA and RSA (default)
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(7) DSA (set your own capabilities)
(8) RSA (set your own capabilities)
(9) ECC and ECC
(10) ECC (sign only)
(11) ECC (set your own capabilities)
(13) Existing key
(14) Existing key from card
Your selection?
```

L'image montre la génération d'une clé RSA de 4096 bits, où l'utilisateur choisit une validité de 1 semaine. Le système affiche la date d'expiration de la clé et demande à l'utilisateur de confirmer ces paramètres.

NB: Ne jamais oublier sa passphrase

```
Please enter the passphrase to
protect your new key
```

```
Passphrase: _____
```

```
<OK>
```

```
<Cancel>
```

### Certificat de révocation

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/8F54A7709D1A6A92F3BE1F8A663BC58373B182A0.rev'
public and secret key created and signed.

pub  rsa4096 2024-09-13 [C] [expires: 2024-09-20]
     8F54A7709D1A6A92F3BE1F8A663BC58373B182A0
uid          oliviers <oliviers@gmail.com>

root@usa-pve:~#
```

### Vérifications préalables

```
gpg -k
```

```
gpg -K
```

## Création des sous-clés , nb : n'oublie pas de la sauvegarder

```

7A1569E43555D0DCFB02430CEA4F13CA1AE169FE
Keygrip = C58EB7E16109995167B2F833C784967169F501A2
uid      [ultimate] DSI-USA (DSI USA <oliviersanhan2016@gmail.com> ») <
oliviersanhan2016@gmail.com>
sub      rsa4096 2024-09-10 [] [expires: 2024-10-10]
Keygrip = 3532EABCA16842B81B11C184CBCE03C0F1A71863
sub      rsa4096 2024-09-13 [SE] [expires: 2024-09-20]
Keygrip = 7D2C78506F0960656E1B60A28E231121D1E5461B
sub      rsa4096 2024-09-13 [] [expires: 2024-09-20]
Keygrip = ACBD2FFE943028D08F1A2026992C7F53E60F7DB8

pub      rsa4096 2024-09-13 [C] [expires: 2024-09-20]
8F54A7709D1A6A92F3BE1F8A663BC58373B182A0
Keygrip = 9C48C78D216AA916F2A4EB49ED634D167C78088D
uid      [ultimate] oliviers <oliviers@gmail.com>

root@usa-pve:~#

```

**NB : Problème** : Vous avez rencontré l'erreur "Could not open a connection to your authentication agent" lorsque vous avez tenté d'utiliser ssh-add -L. Cela signifie que l'agent SSH (ssh-agent) n'était pas en cours d'exécution ou que votre environnement n'était pas correctement configuré pour communiquer avec lui.

**Solution** : Vous avez démarré l'agent SSH avec eval "\$(ssh-agent -s)", ce qui a lancé ssh-agent et configuré votre environnement pour qu'il puisse interagir avec l'agent.

**Problème** : Après avoir démarré l'agent SSH, la commande ssh-add -L indiquait que l'agent n'avait pas d'identités, ce qui signifie qu'aucune clé privée n'avait été ajoutée à l'agent SSH.

**Solution** : Vous avez ajouté votre clé privée à l'agent SSH en utilisant ssh-add ~/.ssh/id\_rsa, ce qui a permis de charger la clé dans l'agent.

**Résultat** : Avec la clé ajoutée, vous devriez maintenant pouvoir vérifier les clés publiques chargées dans l'agent SSH avec ssh-add -L, et vous êtes prêt à utiliser l'agent SSH pour vos connexions sécurisées.

```

root@usa-pve:~# ssh-add -L
Could not open a connection to your authentication agent.
root@usa-pve:~# eval "$(ssh-agent -s)"
Agent pid 2601028
root@usa-pve:~# ssh-add -L
The agent has no identities.
root@usa-pve:~# ssh-add ~/.ssh/id_rsa
Identity added: /root/.ssh/id_rsa (root@usa-pve)
root@usa-pve:~# root@usa-pve:~# ssh-add ~/.ssh/id_rsa
Identity added: /root/.ssh/id_rsa (root@usa-pve)
-bash: root@usa-pve:~#: command not found
-bash: syntax error near unexpected token `('
root@usa-pve:~# ssh-add -L
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDpusQC3tDphhD1LH1YlhVjDaVmhlRULmCJBV49WnAbbXuX/UkR7Lzp
h08Lglh28XfUhaHj7b9VwyeRPBstTjPzPVR9hu3d6NtRMjwSMLvNuJg6FZH9IhtW3X1LCQPHd3Ep0SFgYOMdoUjVSCes
2oBLE6P3hZHRm1Iv2d0k8wIL07LHTkMk/tbkux+idMi4LzbELYFLhfFnmPJbNebWOHiIsF5WeHnLbpXUIETpV6GXehs5
2UBoTh+F5xNZXeov/YRh1SwNxK7tWk6tgjJThSkLMxhMxhHy4pJNCeRP/MshIjh/ZimRxx73HcEvIsscY84bjEmQkAH8
kcZ4HTWQkLBXVuRwjdTL1aHnAvia4PSm9AzUpVtyjweL+/oV00xhA30/GcsLB6iz+nSrHAvrnF222KoB0z0SjblTbd08
SDLMvfqSs1K2ePaHBlgA60LZi8BMwmF/aokPxBgw6VcI78hIFFcDybg67Rdg7J/vqu2DTSDe7B+eER7m0Ay1Cjd0f6n
sw== root@usa-pve

```

## Export / Import de clés

```
root@usa-pve:~/.ssh# gpg --list-secret-keys
/root/.gnupg/pubring.kbx
-----
sec   rsa4096 2024-09-10 [C] [expires: 2024-10-10]
      7A1569E43555D0DCFB02430CEA4F13CA1AE169FE
uid    [ultimate] DSI-USA (DSI USA <oliviersanhan2016@gmail.com>) <oliviersanhan2016@gmail.com>
ssb    rsa4096 2024-09-10 [] [expires: 2024-10-10]
ssb    rsa4096 2024-09-13 [SE] [expires: 2024-09-20]
ssb    rsa4096 2024-09-13 [] [expires: 2024-09-20]

sec   rsa4096 2024-09-13 [C] [expires: 2024-09-20]
      8F54A7709D1A6A92F3BE1F8A663BC58373B182A0
uid    [ultimate] oliviers <oliviers@gmail.com>

root@usa-pve:~/.ssh# gpg -a --export-secret-keys 7A1569E43555D0DCFB02430CEA4F13CA1AE169FE > secret.asc
root@usa-pve:~/.ssh# gpg -a --export-secret-keys 8F54A7709D1A6A92F3BE1F8A663BC58373B182A0 > secret.asc
root@usa-pve:~/.ssh# source .bash_profile
-bash: .bash_profile: No such file or directory
root@usa-pve:~/.ssh# cat secret.asc
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQdGBGbj3U4BEADLrYd8H5sTwagnqZk5FLEQyrIweHnviLqRiAPvkr4gSk90jYFc
3bHrfoPue370p1QDCroZ0y7mon/R81Bd+ao3Mtm+J4TKq4XFkz1DHnt0lF4sZo+
GvhFS8RksCIduo0Cg4ISax+NNjW0gu75dZ7wuGKSCysHZwWV2iD1zrQCn3YiXT
qbth/ES4wGDwWV8GortPM1nRXeupID9DvstIRe5SookH4P/PBP1hZstJXnc1bdWx
```

- Chiffrer/Déchiffrer un document

```
root@usa-pve:~# gpg --import /root/public_key.asc
```

gpg: key A0538B4921C5BEDA: public key "Florent Sautour [sautour@beaupeyrat.com](mailto:sautour@beaupeyrat.com)" imported gpg:  
Total number processed: 1 gpg: imported: 1

From:

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

Permanent link:

[https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:pgp\\_-\\_pgp](https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:pgp_-_pgp)

Last update: **2024/09/17 15:24**

