110.3 GNUPG (3/2)

Voir Aussi

- Le manuel de GnuPG
- Utilisation de GPG — Linux France
- Wikibook GPG (fr)
- man gnupg

~/.gnupg/

- OPTIONS PAR DÉFAUT : gpg.conf
- CLÉS PUBLIQUES — TROUSSEAU : pubring.gpg
- random_seed
- CLÉS PRIVÉES — TROUSSEAU : secring.gpg
- BASE DE CONFIANCE : trustdb.gpg

GNU Privacy Guard

- CF PGP : Pretty Good Privacy
- IMPLÉMENTATION : OPENPGP — RFC2440
- ⚠ PAIRE DE CLÉS : PRIVÉE / PUBLIQUE
- ⚠ CHAÎNE DE CONFIANCE
- OBJECTIFS : SIGNER / CHIFFRER / FICHIERS : EMAIL / DOCUMENT
- DIFFUSION — SERVEURS : pgp.mit.edu / ...

DOCUMENTS

CHIFFRER
```
gpg -e | --encrypt
gpg -e -u "Prénom Nom"  \
  -r "Lecteur" fichier.txt
```

DÉCHIFFRER
```
gpg -d | --decrypt
gpg -d fichier.txt.gpg
```

SIGNER
```
gpg --sign doc
gpg --output doc.sig --sign doc
```
EN CLAIR : `gpg --clearsign doc`

VÉRIFIER
```
gpg --verify doc.sig
```

CLÉS

GÉNÉRER
```
gpg --gen-key
```

ENVOYER
```
gpg --keyserver pgp.mit.edu
  --send-keys nom@domaine
```

ÉCHANGE

LISTER
```
gpg --list-keys   (gpg -k)
gpg --list-sigs
```

EXPORTER

PUBLIQUE :
```
gpg --armor \
  --export nom@domaine        → ASCII
gpg --output nom.gpg \
  --export nom@domaine        → BINAIRE
```

PRIVÉE :
```
gpg --export-secret-key \
  -a "Prénom Nom" \
  -o private.key
```

LES DEUX :
```
gpg --export -o sauve
```

IMPORTER
```
gpg --import nom.gpg
gpg --recv-keys ABCD0123
gpgp --delete-keys ABCD0123
```

SIGNER
```
gpg --edit-key nom@domaine
  Command> sign
  Command> trust
  Command> check
```

RÉVOQUER

GÉNÉRER :
```
gpg --output revoke.asc --gen-revoke
  mykey
gpg --gen-revoke nom@domaine >
  revoke_key.txt
```

PRISE EN COMPTE :
```
gpg –import revoke.asc
```

SUPPRIMER
```
gpg –delete-secret-keys nom@domaine
gpg –delete-keys nom@domaine
```

UTILISATION