GNU Privacy Guard (GPG)

Índex

GNU Privacy Guard (GPG o GnuPG) és una implementació lliure i de codi obert de l'estàndard **OpenPGP** (RFC 4880). Permet xifrar i signar dades i comunicacions, gestionar claus criptogràfiques i verificar l'autenticitat de fitxers i missatges.

Figura 1: GnuPG logo

1. Història i origen

- L'estàndard **PGP** (Pretty Good Privacy) va ser creat per **Phil Zimmermann** el **1991**.
- PGP va ser adquirit per diverses empreses (ViaCrypt, Network Associates, PGP Corporation, Symantec, finalment Broadcom).
- El **1997**, la IETF va estandarditzar PGP com a **OpenPGP** (RFC 2440, actualitzat a RFC 4880 el 2007).
- **Werner Koch** va iniciar GnuPG el **1997** com a alternativa lliure a PGP.
- La versió **1.0.0** va ser publicada el **1999**.
- GnuPG està escrit en **C** i distribuït sota la llicència **GPL v3**.
- És mantingut per la **Free Software Foundation** i per Koch a través de g10 Code GmbH.
- El 2015 una campanya de finançament col·lectiu va recaptar 250.000 € per garantir-ne el manteniment continuat.

2. Estàndards i protocols

Estàndard	Descripció
OpenPGP	RFC 4880 --- format de missatges, claus i signatures
RFC 4880bis	Esborrany d'actualització (ed25519, AEAD)
S/MIME	GPG pot interoperar amb S/MIME via `gpgsm`
X.509	Suportat via `gpgsm` per a certificats de CA
SSH	L'agent GPG pot substituir `ssh-agent`

3. Versions principals de GnuPG

Versió	Estat	Notes
GnuPG 1.x (`gpg`)	Llegat	Monolític, sense dependències externes
GnuPG 2.x (`gpg2`)	Actual	Modular, amb `gpg-agent`, suport a smartcards
GnuPG 2.2.x	LTS	Branca estable de llarg suport
GnuPG 2.4.x	Modern	Branca més recent, millores en ed25519, AEAD

A la majoria de distribucions actuals, `gpg` és un àlies de `gpg2`.

4. Components del paquet GnuPG

Component	Descripció
`gpg`	Eina principal per a OpenPGP
`gpg2`	Versió modular (equivalent a `gpg` en sistemes moderns)
`gpg-agent`	Dimoni que gestiona les claus privades i frases de pas
`gpgsm`	Gestió de certificats S/MIME i X.509
`gpgconf`	Configuració dels components de GnuPG
`gpg-connect-agent`	Comunicació directa amb `gpg-agent`
`dirmngr`	Dimoni per accedir a servidors de claus i CRL/OCSP
`scdaemon`	Gestió de smartcards i tokens USB (YubiKey, etc.)
`gpgtar`	Xifratge i signatura d'arxius tar
`watchgnupg`	Monitoratge dels sockets de GnuPG

5. Instal·lació

Debian / Ubuntu

```
sudo apt update
sudo apt install gnupg2
```

Fedora / RHEL

```
sudo dnf install gnupg2
```

Arch Linux / Manjaro

```
sudo pacman -S gnupg
```

macOS (via Homebrew)

```
brew install gnupg
```

Windows

Descarregar **Gpg4win** des de https://gpg4win.org (inclou Kleopatra com a interfície gràfica).

6. Conceptes criptogràfics fonamentals

6.1. Criptografia asimètrica (clau pública/privada)

- Cada usuari té un **parell de claus:** una **clau pública** (compartida) i una **clau privada** (secreta).
- Qualsevol pot **xifrar** un missatge amb la clau pública del destinatari.
- Només el propietari de la **clau privada** pot desxifrar-lo.
- La **signatura digital** s'obté xifrant un hash del missatge amb la clau privada; qualsevol amb la clau pública pot verificar-la.

6.2. Web of Trust (Xarxa de Confiança)

GPG no usa una autoritat de certificació centralitzada (CA), sinó una **xarxa de confiança descentralitzada**:

- Els usuaris signen les claus d'altri per atestar la seva autenticitat.
- La confiança es propaga a través de la xarxa.
- Nivells de confiança: `unknown`, `none`, `marginal`, `full`, `ultimate`.

6.3. Nivells de validesa d'una clau

Validesa	Descripció
`unknown`	No se sap res de la clau
`undefined`	No s'ha assignat confiança
`marginal`	Confiança parcial
`full`	Confiança plena
`ultimate`	Confiança absoluta (pròpies claus)

7. Algoritmes suportats

7.1. Xifratge simètric

`AES-128`, `AES-192`, `AES-256`, `3DES`, `CAST5`, `Blowfish`, `Twofish`, `Camellia`

7.2. Xifratge asimètric

`RSA`, `DSA`, `ElGamal`, `ECDH`, `ECDSA`, `EdDSA (Ed25519)`

7.3. Hash / Resum

`SHA-1`, `SHA-256`, `SHA-384`, `SHA-512`, `SHA-224`, `RIPEMD-160`, `MD5`

7.4. Recomanacions actuals (2024)

- Clau: **Ed25519** per a signar, **Curve25519 (ECDH)** per a xifrar
- Hash: **SHA-256** o superior
- Xifratge simètric: **AES-256**
- Mida mínima RSA recomanada: **3072 bits** (millor 4096)

8. Gestió de claus

8.1. Generar un parell de claus

```
# Generació interactiva (recomanada)
gpg --full-generate-key

# Generació ràpida amb valors per defecte
gpg --gen-key

# Generació per lots (no interactiva)
gpg --batch --generate-key <<EOF
%echo Generant clau de prova
Key-Type: EdDSA
Key-Curve: Ed25519
Subkey-Type: ECDH
Subkey-Curve: Curve25519
Name-Real: Ramon López
Name-Email: ramon@thosicodina.cat
Expire-Date: 2y
Passphrase: la_meva_frase_de_pas
%commit
EOF
```

8.2. Llistar claus

```
# Claus públiques del clauer
gpg --list-keys
gpg -k

# Claus privades del clauer
gpg --list-secret-keys
gpg -K

# Amb empremtes digitals (fingerprints)
gpg --list-keys --fingerprint
```

```
# Format llarg (amb KeyID complet de 16 hex)
gpg --list-keys --keyid-format LONG
```

8.3. Exportar claus

```
# Exportar clau pública (format ASCII)
gpg --armor --export ramon@thosicodina.cat > clau_publica.asc

# Exportar clau privada (fer còpia de seguretat!)
gpg --armor --export-secret-keys ramon@thosicodina.cat >
 ↪  clau_privada.asc

# Exportar subclaus privades
gpg --armor --export-secret-subkeys ramon@thosicodina.cat >
 ↪  subclaus.asc
```

8.4. Importar claus

```
# Importar una clau pública
gpg --import clau_publica.asc

# Importar des d'un servidor de claus
gpg --keyserver hkps://keys.openpgp.org --recv-keys 0xIDDELACLAU
```

8.5. Eliminar claus

```
# Eliminar clau pública (cal eliminar primer la privada si n'hi ha)
gpg --delete-key ramon@thosicodina.cat

# Eliminar clau privada
gpg --delete-secret-key ramon@thosicodina.cat

# Eliminar ambdues
gpg --delete-secret-and-public-key ramon@thosicodina.cat
```

8.6. Editar una clau

```
gpg --edit-key ramon@thosicodina.cat
```

Subordres útils dins `gpg --edit-key`:

Subordre	Acció
`passwd`	Canvia la frase de pas
`expire`	Canvia la data de caducitat
`adduid`	Afegeix una identitat (UID)
`deluid`	Elimina una identitat
`addsubkey`	Afegeix una subclau
`revuid`	Revoca una identitat
`trust`	Assigna nivell de confiança
`sign`	Signa la clau
`save`	Desa els canvis
`quit`	Surt sense desar

9. Xifratge i desxifratge

9.1. Xifrar un fitxer per a un destinatari

```
# Xifratge asimètric (per al destinatari)
gpg --encrypt --recipient destinatari@thosicodina.cat document.pdf

# Xifratge per a múltiples destinataris
gpg -e -r destinatari1@thosicodina.cat -r
 ↪  destinatari2@thosicodina.cat fitxer.txt

# Xifratge + signatura en un sol pas
gpg --encrypt --sign --recipient destinatari@thosicodina.cat
 ↪  fitxer.txt

# Sortida en format ASCII (armored)
gpg --armor --encrypt -r destinatari@thosicodina.cat fitxer.txt
# Genera fitxer.txt.asc
```

9.2. Xifratge simètric (amb contrasenya)

```
# Xifratge simètric (demanarà una contrasenya)
gpg --symmetric fitxer.txt
# Genera fitxer.txt.gpg

# Especificant algoritme
gpg --symmetric --cipher-algo AES256 fitxer.txt

# Amb sortida ASCII
gpg --armor --symmetric fitxer.txt
```

9.3. Desxifratge

```
# Desxifratge (detecta automàticament el tipus)
gpg --decrypt fitxer.txt.gpg > fitxer_desxifrat.txt

# O simplement
gpg fitxer.txt.gpg
```

10. Signatures digitals

10.1. Signar un fitxer

```
# Signatura separada (crea fitxer.txt.sig)
gpg --detach-sign fitxer.txt

# Signatura separada en ASCII
gpg --armor --detach-sign fitxer.txt
# Crea fitxer.txt.asc

# Signatura integrada (crea fitxer.txt.gpg amb contingut + signatura)
gpg --sign fitxer.txt

# Signatura de text en clar (llegible sense GPG, signatura al peu)
gpg --clearsign fitxer.txt
# Crea fitxer.txt.asc
```

10.2. Verificar una signatura

```
# Verificar signatura separada
gpg --verify fitxer.txt.asc fitxer.txt

# Verificar signatura integrada o en clar
gpg --verify fitxer.txt.gpg

# Verificar i extreure el contingut
gpg --output fitxer_original.txt --decrypt fitxer.txt.gpg
```

10.3. Exemple de sortida de verificació correcta

```
gpg: Signature made dl 08 jun 2026 10:30:00 CEST
gpg:                using EdDSA key A1B2C3D4E5F60001
gpg: Good signature from "Ramon López <ramon@thosicodina.cat>"
 ↪  [ultimate]
```

11. Certificats de revocació

És **imprescindible** generar el certificat de revocació just després de crear la clau.

```
# Generar certificat de revocació
gpg --gen-revoke ramon@thosicodina.cat > revocacio.asc

# Aplicar la revocació (quan calgui)
gpg --import revocacio.asc

# Publicar la revocació al servidor de claus
gpg --keyserver hkps://keys.openpgp.org --send-keys 0xIDDELACLAU
```

> **Important:** Desa el fitxer de revocació en un lloc segur i separat de la clau privada.

12. Servidors de claus

```
# Pujar clau pública a un servidor
gpg --keyserver hkps://keys.openpgp.org --send-keys 0xIDDELACLAU

# Buscar una clau per correu
gpg --keyserver hkps://keys.openpgp.org --search-keys
 ↪  usuari@exemple.com

# Baixar/actualitzar una clau
gpg --keyserver hkps://keys.openpgp.org --recv-keys 0xIDDELACLAU

# Actualitzar totes les claus del clauer
gpg --refresh-keys
```

12.1. Servidors de claus populars

Servidor	Notes
`hkps://keys.openpgp.org`	Recomanat; verifica propietat per correu
`hkps://keyserver.ubuntu.com`	Mantingut per Canonical
`hkps://pgp.mit.edu`	Històric, no suprimeix claus
`hkps://keys.mailvelope.com`	Usat per Mailvelope

13. GPG-Agent

`gpg-agent` és un dimoni que guarda les frases de pas en memòria durant una sessió, evitant haver-les d'introduir repetidament.

```
# Iniciar l'agent (normalment s'inicia automàticament)
gpg-agent --daemon

# Verificar que l'agent corre
gpg-connect-agent /bye

# Oblidar totes les frases de pas en caché
gpg-connect-agent reloadagent /bye

# Configuració: ~/.gnupg/gpg-agent.conf
default-cache-ttl 3600      # Temps de caché en segons (1h)
max-cache-ttl 86400         # Temps màxim (24h)
pinentry-program /usr/bin/pinentry-gtk-2  # Programa per demanar frase
 ↪  de pas
```

13.1. GPG-Agent com a SSH-Agent

```
# Afegir a ~/.gnupg/gpg-agent.conf
enable-ssh-support

# Afegir a ~/.bashrc o ~/.zshrc
export SSH_AUTH_SOCK=$(gpgconf --list-dirs agent-ssh-socket)
gpgconf --launch gpg-agent
```

14. Subclaus

Les **subclaus** permeten mantenir la clau mestra (certificació) fora de línia i usar subclaus per a les operacions quotidianes.

Estructura recomanada:

```
Clau mestra [C] --- Certificació (offline, molt protegida)
├── Subclau [S] --- Signatura
├── Subclau [E] --- Xifrat
└── Subclau [A] --- Autenticació (SSH)
```

```
# Afegir subclau a una clau existent
gpg --edit-key ramon@thosicodina.cat
> addsubkey
# Seleccionar tipus (sign/encrypt/auth) i mida/corba
> save
```

15. Smartcards i YubiKey

GnuPG suporta targetes intel·ligents via `scdaemon`:

```
# Llistar targetes connectades
gpg --card-status

# Moure subclaus a la targeta (operació irreversible!)
gpg --edit-key ramon@thosicodina.cat
> key 1
> keytocard
> save

# Configurar PIN de la targeta
gpg --card-edit
> passwd
```

YubiKey és el dispositiu més popular per a aquest ús (OpenPGP Card 3.x).

16. Configuració avançada

16.1. Fitxer `~/.gnupg/gpg.conf`

```
# Algoritmes preferits
personal-cipher-preferences AES256 AES192 AES
personal-digest-preferences SHA512 SHA384 SHA256
personal-compress-preferences ZLIB BZIP2 ZIP Uncompressed

# Format d'identificació de claus llarg
keyid-format LONG

# Mostrar empremtes digitals
with-fingerprint

# Servidor de claus per defecte
keyserver hkps://keys.openpgp.org

# No incloure la versió als fitxers armored
no-emit-version

# Xifratge creusat (per a un mateix)
default-recipient-self

# No incluir comentaris
no-comments

# Hash per defecte
cert-digest-algo SHA512
```

17. Integració amb aplicacions

17.1. Correu electrònic

Client	Integració
Thunderbird	Suport natiu OpenPGP des de v78
Mutt/NeoMutt	Integrat per defecte
Evolution	Connector GPG integrat
KMail	Connector Kleopatra (KDE)
Geary	Suport bàsic

17.2. Navegadors web

- **Mailvelope**: extensió per a Chrome/Firefox per a Gmail, Yahoo Mail, Outlook
- **FlowCrypt**: extensió per a Gmail

17.3. Gestors de contrasenyes

- **pass** (password-store): gestor de contrasenyes en CLI que usa GPG per xifrar cada entrada.

```
sudo apt install pass
pass init ramon@thosicodina.cat
pass insert correu/gmail
pass show correu/gmail
```

17.4. Git --- Signatura de commits

```
# Configurar GPG per a Git
git config --global user.signingkey 0xIDDELACLAU
git config --global commit.gpgsign true
git config --global gpg.program gpg2

# Commit signat
git commit -S -m "Commit amb signatura GPG"

# Verificar signatura d'un commit
git log --show-signature
git verify-commit HEAD
```

17.5. Paquets de distribucions Linux

GPG s'usa per verificar l'autenticitat dels dipòsits:

```
# Debian/Ubuntu: claus dels dipòsits a /etc/apt/trusted.gpg.d/
# Verificar un paquet descarregat
gpg --verify paquet.deb.asc paquet.deb
```

18. Casos d'ús pràctics

18.1. Xifrar còpies de seguretat

```
# Xifrar un tar amb GPG
tar czf - /home/usuari/ | gpg --symmetric --cipher-algo AES256 -o
 ↪  backup.tar.gz.gpg

# Desxifrar i restaurar
gpg -d backup.tar.gz.gpg | tar xzf - -C /destí/
```

18.2. Verificar integritat d'una ISO

```
# Baixar la clau del projecte
gpg --keyserver hkps://keys.openpgp.org --recv-keys 0xCLAUDELPROJECTE

# Verificar
gpg --verify ubuntu-24.04.iso.gpg ubuntu-24.04.iso
```

18.3 Xifrar i signar un fitxer alhora

```
gpg --encrypt --sign --armor \
    --recipient destinatari@thosicodina.cat \
    --local-user jo@thosicodina.cat \
    fitxer_confidencial.txt
```

19. Bones pràctiques de seguretat

1. **Usa una frase de pas forta** per protegir la clau privada.
2. **Genera un certificat de revocació** immediatament i guarda'l fora de línia.
3. **Fes còpies de seguretat** de la clau privada en un lloc segur (USB xifrat, paper).
4. **Usa subclaus** per a les operacions diàries; mantén la clau mestra fora de línia.
5. **Estableix data de caducitat** (1--2 anys recomanats); es pot renovar.
6. **Verifica les empremtes digitals** de les claus per un canal independent.
7. **Actualitza regularment** les claus dels contactes (`gpg --refresh-keys`).
8. **Usa algoritmes moderns**: Ed25519/Curve25519 en lloc de RSA-2048 antic.
9. **Protegeix `~/.gnupg/`**: permisos `700` al directori, `600` als fitxers.
10. **No confies en claus no verificades**: la Web of Trust requereix verificació física o per múltiples canals.

```
# Permisos correctes
chmod 700 ~/.gnupg
chmod 600 ~/.gnupg/*
```

20. Directori de treball i fitxers importants

Ruta	Contingut
`~/.gnupg/`	Directori principal de GnuPG
`~/.gnupg/pubring.kbx`	Clauer públic (format KeyBox, GnuPG >= 2.1)
`~/.gnupg/trustdb.gpg`	Base de dades de confiança
`~/.gnupg/private-keys-v1.d/`	Claus privades (una per fitxer)
`~/.gnupg/gpg.conf`	Configuració de GPG
`~/.gnupg/gpg-agent.conf`	Configuració de l'agent
`~/.gnupg/dirmngr.conf`	Configuració del gestor de directoris
`~/.gnupg/sshcontrol`	Claus autoritzades per SSH via GPG-Agent

21. Resolució de problemes habituals

L'agent no respon

```
gpgconf --kill gpg-agent
gpg-agent --daemon
```

“No public key” en verificar

```
gpg --keyserver hkps://keys.openpgp.org --recv-keys 0xIDDELACLAU
```

Permisos incorrectes

```
gpgconf --check-dirs
chmod 700 ~/.gnupg && chmod 600 ~/.gnupg/*
```

Clau expirada (renovar)

```
gpg --edit-key ramon@thosicodina.cat
> expire
# Introduir nova durada (p. ex. "2y")
> save
gpg --keyserver hkps://keys.openpgp.org --send-keys 0xIDDELACLAU
```

Veure informació detallada d'una clau

```
gpg --list-packets fitxer.asc
gpg --verbose --list-keys ramon@thosicodina.cat
```

22. Alternatives i eines relacionades

Eina	Descripció
Age	Eina moderna de xifratge de fitxers, sintaxi senzilla
Sequoia-PGP	Implementació OpenPGP en Rust
Kleopatra	Interfície gràfica per a GnuPG (KDE/Windows)
GPG Suite	Integració de GPG per a macOS
Gpg4win	Paquet GPG per a Windows (inclou Kleopatra)
pass	Gestor de contrasenyes basat en GPG
gopass	Alternativa moderna a `pass`

23. Recursos oficials

- **Web oficial:** https://gnupg.org
- **Documentació:** https://gnupg.org/documentation/
- **Manual complet:** https://www.gnupg.org/gph/en/manual.html
- **Codi font:** https://git.gnupg.org
- **RFC 4880 (OpenPGP):** https://tools.ietf.org/html/rfc4880
- **Llista de correu:** https://lists.gnupg.org

Versions d'aquest document

- HTML - gpg.html
- PDF - gpg.pdf
- ODT - gpg.odt
- MD - gpg.md