Git-Secret with GPG - Full Setup Documentation

==========

Step 1: Generate a GPG Key Pair

$ gpg --full-generate-key

Choose:

- Key type: RSA and RSA

- Key size: 4096

- Expiry: 0 (never expires)

- Name and email

- Passphrase (optional)

Validate the key:

$ gpg --list-secret-keys --keyid-format LONG

Step 2: Initialize git-secret in your repo

$ cd your-git-repo

$ git secret init

Step 3: Add your GPG key to git-secret

$ git secret tell you@example.com

Verify:

$ git secret whoknows

Step 4: Add files to encrypt

$ echo "API_KEY=supersecret" > mysecrets.env

$ git secret add mysecrets.env

$ git secret list

Step 5: Encrypt secret files

$ git secret hide

(creates mysecrets.env.secret)

Step 6: Ignore original files

$ echo "mysecrets.env" >> .gitignore

$ git add .

$ git commit -m "Add encrypted secrets"

$ git push

Step 7: Decrypt secrets

$ git secret reveal

Step 8: Export private key for CI/CD

$ gpg --armor --export-secret-keys you@example.com > privatekey.asc

Pipeline Import (example):

$ echo "$GPG_PRIVATE_KEY" | gpg --batch --import

$ git secret reveal

Validation Checklist

- gpg --list-secret-keys # Shows your key
- git secret whoknows # Shows allowed users
- git secret list # Lists tracked secrets
- git secret hide/reveal # Encrypts/decrypts