GNUPG: Best Practices

Configuration of GNUPG

Configuration

- Use HKPS for secure SSL connection to the keyserver

Configuration of GNUPG

Configuration

- Use HKPS for secure SSL connection to the keyserver
- Use a keyserver pool like hkps://hkps.pool.sks-keyservers.net

Configuration of GNUPG

Configuration

- Use HKPS for secure SSL connection to the keyserver
- Use a keyserver pool like hkps://hkps.pool.sks-keyservers.net
- Use the full fingerprint and not only the short keyid

Configuration of GNUPG

Configuration

- Use HKPS for secure SSL connection to the keyserver
- Use a keyserver pool like hkps://hkps.pool.sks-keyservers.net
- Use the full fingerprint and not only the short keyid
- Use secure digest methods for key creation and signatures

Generate key

Key generation:

- Choose a secure algoritym like RSA for your signing and encrytion keys

Generate key

Key generation:

- Choose a secure algoritym like RSA for your signing and encrytion keys
- Use a long keysize like 4096 bit

Generate key

Key generation:

- Choose a secure algoritym like RSA for your signing and encrytion keys
- Use a long keysize like 4096 bit
- Set an expiry date that is not so far in the future, like 1 year

Generate key

Key generation:

- Choose a secure algoritym like RSA for your signing and encrytion keys
- Use a long keysize like 4096 bit
- Set an expiry date that is not so far in the future, like 1 year
- A key uid consists of your real name and an email address only you control

Generate key

Key generation:

- Choose a secure algoritym like RSA for your signing and encrytion keys
- Use a long keysize like 4096 bit
- Set an expiry date that is not so far in the future, like 1 year
- A key uid consists of your real name and an email address only you control
- Leave the comment field empty

Generate key

Key generation:

- Choose a secure algoritym like RSA for your signing and encrytion keys
- Use a long keysize like 4096 bit
- Set an expiry date that is not so far in the future, like 1 year
- A key uid consists of your real name and an email address only you control
- Leave the comment field empty
- Choose a strong passphrase

Add another uid

Manage uids

- Add uids to your key

Add another uid

Manage uids

- Add uids to your key
- Iff you use xmpp you can add a comment that you do not receive email on that uid

Add another uid

Manage uids

- Add uids to your key
- Iff you use xmpp you can add a comment that you do not receive email on that uid
- You can set a later added uid as primary uid

Secure yourself against identity theft or key loss

Generate revocation certificate

- generate the revocation certificate, so that you can revoke a compromised or lost key
- keep it in a safe place

Key rollover

Getting rid of the old key and communicating the new one

- Sign your new key with your old one

Key rollover

Getting rid of the old key and communicating the new one

- Sign your new key with your old one
- Upload your new key to the key servers

Key rollover

Getting rid of the old key and communicating the new one

- Sign your new key with your old one
- Upload your new key to the key servers
- Inform others that you have changed your key

Storage of private key and revocation certificate

Do not lose your keys

- Encrypt your hard drive

Storage of private key and revocation certificate

Do not lose your keys

- Encrypt your hard drive
- Do backups on a regular basis

Storage of private key and revocation certificate

Do not lose your keys

- Encrypt your hard drive
- Do backups on a regular basis
- Encrypt your backups

Storage of private key and revocation certificate

Do not lose your keys

- Encrypt your hard drive
- Do backups on a regular basis
- Encrypt your backups
- Use tools like gfshare

Literature

1. OpenPGP Best Practices
2. Key-Rollover
3. libgfshare
4. Writing beamer presentations in org-mode
5. Org-mode: Beamer Export

License