GNUPG: Best Practices

1 Cheat Sheet

1.1 Configuration of gpg

1.1.1 Configuration of GNUPG

1. ~/.gnupg/gpg.conf

```
# when outputting certificates, view user IDs distinctly from keys:
fixed-list-mode
# long keyids are more collision-resistant than short keyids
keyid-format 0xlong
# choose the strongest digest:
personal-digest-preferences SHA512 SHA384 SHA256 SHA224
# preferences for new keys:
default-preference-list SHA512 SHA384 SHA256 SHA224 AES256 AES192 \
                        AES CAST5 BZIP2 ZLIB ZIP Uncompressed
# use gpg-agent
use-agent
# show which User IDs gpg thinks are bound to keys in the keyring:
verify-options show-uid-validity
list-options show-uid-validity
# for OpenPGP certification, use a strong digest:
cert-digest-algo SHA256
```

1.2 Generation of keys and key rollover

1.2.1 Generate key

1. gpg `--gen-key`:
    - Choose RSA and RSA
    - Keysize 4096

- Expires 1y
- Real Name: Alice Mustermann
- Email address: 1musterm@inf
- Comment: leave empty
- Passphrase: type in a strong passphrase

1.2.2 Add another uid and set primary uid

1. gpg `--edit-key 0x12345678`:
   - adduid
   - Real name: Alice Mustermann
   - Email address: 01musterm@jabber.mafiasi.de
   - Comment: XMPP / DO NOT USE FOR EMAIL
   - save
2. gpg `--edit-key 0x12345678`:
   - uid 3
   - primary
   - save

1.2.3 Generate revocation certificate

1. gpg `--output revoke-0x12345678.asc --gen-revoke 0x12345678`
   - generate the revocation certificate, so that you can revoke a compromised or lost key
   - keep it in a safe place

1.2.4 Key rollover: Sign my new key with my old key

1. Sign key:
   - gpg `--default-key 0x01d12345 --sign-key 0x12345678`
2. Upload key to web of trust:
   - gpg `--send-key 0x12345678`

1.3 Keep your private key secure

1.3.1 Storage of private key and revocation certificate

1. GFshare
    - share the private key between devices
    - split the key in 5 parts with gfsplit
    - use 1 pen drive for 2 parts of the key
    - use 3 other locations for each 1 part of the key
    - you need 3 parts to reconstruct the key with gfcombine

2 Sources & Documentation

2.1 Weblinks

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

3 License