How to generate a GPG Key with multiple uids & subkeys?



This page is still a DRAFT.

Requirements

Disk Image

Download the latest Arch Linux or ArchBang Linux release and write it to a bootable CD or USB thumbdrive.

<sxh bash;gutter: false> ~$: dd if=archlinux-$VERSION-dual.iso of=/dev/$DEVICE bs=8192 </sxh>

Than boot your computer with it.



Paranoid Modus: use a **non-networked** computer for this procedure.

Effectively preventing pinentry from failing

```
gpg: problem with the agent: No pinentry
```

<sxh bash;gutter: false> ~$: echo "pinentry-program `which pinentry-tty`" » ./.gnupg/gpg-agent.conf </sxh>

Generating the master key

<sxh bash;gutter: false> ~$: gpg2 –expert –full-gen-key # 10 # 1 # 0 # y # Real NAME # E-Mail Address # Comment # O # y # T </sxh>

Generating the sub keys to your master key

<sxh bash;gutter: false> ~$: gpg2 --expert --edit-key $KEYID gpg> addkey # 8 # Q # 4096 # 1y # y # y # T gpg> save </sxh>

Removing the primary key

<sxh bash;gutter: false> ~$: gpg -K ~$: gpg -a --export-secret-subkeys $KEYID > 0x$KEYID-secret.subkeys.gpg ~$: gpg --delete-secret-keys $KEYID # y # y # D # D # D </sxh>

Troubleshooting

Error while generating key?

If you get the following error while the key generation:

```
gpg: can't connect to the agent: IPC connect call failed
gpg: agent_genkey failed: No agent running
Key generation failed: No agent running
```

it means your gpg-agent isn't running.

FAQ

1. Why using Arch*Linux instead of something more security related like Tails?

In the moment of writing, Tails doesn't include the latest gpg2 package within its distribution. To narrow down as much obstacles as possible, I've chosen a distribution which includes all needed software packages.

References

Further Reading

- FSDE - E-Mail Defense Guide (Beginner's Guide & visually addressing)
- Debian Wiki - Creating a new GPG key
- Debian Wiki - Subkeys
- Generating More Secure GPG Keys: A Step-by-Step Guide
- GPG KeyGenerator (An online service generating GPG keys within your browser. Advertised as secure and trustworthy, though not recommended.)
- Annoyances and How-Tos: “gpg: problem with the agent: No pinentry” — SOLVED
- Hauke Laging - GnuPG subkeys
- gniibe - Creating newer ECC keys for GnuPG
- Creating the perfect GPG keypair
- Creating a new GPG key with subkeys
- Anomalies when importing keyring to gpg

From:
https://wiki.c3l.lu/ - **Chaos Computer Club Lëtzebuerg**

Permanent link:
https://wiki.c3l.lu/doku.php?id=projects:howtos:gpg&rev=1455292030

Last update: **2016/02/12 16:47**