Je PGP-hoofdsleutel offline bewaren

Versleutelde microSD-back-up onder Ubuntu — met f3-echtheidscheck en paperkey

Auteur	Datum	Versie	Systeem	Publicatie
Patrick	**Juli 2026**	**v1.0**	**Ubuntu / GnuPG**	**nell.quest**

> **Waar het om gaat.** Je PGP-hoofdsleutel (Certify-key) hoort niet op je alledaagse computer, maar offline. Deze handleiding bewaart hem op twee versleutelde microSD-kaarten — idealiter van twee verschillende winkels — plus een papieren afdruk als langetermijnanker. Voer elke stap voor **beide kaarten** apart uit. Alle commando's zijn om te kopiëren.

0. Gereedschap installeren

```
sudo apt update
sudo apt install f3 cryptsetup paperkey
```

1. De kaart identificeren — de gevaarlijke stap

```
lsblk
```

Vind je kaart op basis van de **grootte** (bijv. 29–30 GiB bij een 32-GB-kaart). Ze heet bijv. `/dev/sdb`.

> ⚠ **Onthoud deze naam precies.** Alle volgende commando's wissen het doelapparaat. Eén verkeerde letter = je systeemschijf is weg. Vervang hieronder `/dev/sdX` consequent door de echte naam.

2. Echtheidscheck met f3

Deze test schrijft de kaart vol en meet de **echte** capaciteit — zo ontmasker je vervalste „32 GB" die in werkelijkheid minder bevatten:

```
sudo f3probe --destructive --time-ops /dev/sdX
```

Meldt hij `Good news: The device is genuine` met de juiste grootte → alles in orde.

> **Als `f3probe` ontbreekt** (in het Ubuntu-pakket zitten soms alleen `f3write` / `f3read`): formatteer de kaart kort met FAT, koppel hem aan, en gebruik dan `f3write /mnt/test` gevolgd door `f3read /mnt/test`. Daarna overschrijf je hem voor stap 3 toch weer.

3. LUKS-versleuteling aanmaken

```
sudo cryptsetup luksFormat /dev/sdX
```

Typ `YES` (hoofdletters) en kies een **sterke wachtwoordzin** (2×).

> ⚠ **Deze wachtwoordzin beschermt je hoofdsleutel.** Verlies je hem, dan is de back-up onbruikbaar. Bewaar hem in Proton Pass — niet op dezelfde kaart.

Container openen en formatteren:

```
sudo cryptsetup open /dev/sdX keybackup
sudo mkfs.ext4 /dev/mapper/keybackup
sudo mkdir -p /mnt/keybackup
sudo mount /dev/mapper/keybackup /mnt/keybackup
```

(ext4 is ideaal als je alleen Linux gebruikt. Moet de kaart ook onder Windows leesbaar zijn: `mkfs.exfat` in plaats van ext4.)

4. Sleutelmateriaal exporteren

Het schoonst werk je in het RAM-geheugen, zodat er niets op je systeemschijf achterblijft:

```
mkdir -p /dev/shm/keywork && cd /dev/shm/keywork

gpg --export-secret-keys -a JOUW@ADRES > PRIVE_VOLLEDIG.asc
gpg --export -a JOUW@ADRES             > PUBLIEK.asc
```

Het intrekkingscertificaat staat al klaar:

```
cp ~/.gnupg/openpgp-revocs.d/*.rev .
```

5. paperkey-afdruk maken — het langetermijnanker

`paperkey` haalt alleen de geheime delen eruit (compact, afdrukbaar):

```
gpg --export-secret-keys JOUW@ADRES > masterkey-secret.gpg
paperkey --secret-key masterkey-secret.gpg --output masterkey-paperkey.txt
```

`masterkey-paperkey.txt` is het bestand om **af te drukken**.

> ⚠ **Druk af op een lokaal aangesloten printer**, niet via een netwerk- of cloudprinter — anders is de printopdracht een lek. Maak 2 afdrukken voor 2 locaties.

6. Naar de versleutelde kaart kopiëren

```
sudo cp PRIVE_VOLLEDIG.asc PUBLIEK.asc *.rev masterkey-paperkey.txt /mnt/keybackup/
sync
```

Op de kaart horen: geheime sleutel, publieke sleutel, intrekkingscertificaat — en optioneel de paperkey-tekst als digitale kopie.

7. Netjes afsluiten

```
sudo umount /mnt/keybackup
sudo cryptsetup close keybackup
```

Werkkopieën in RAM verdwijnen vanzelf bij een herstart. Voor de zekerheid meteen:

```
cd ~ && rm -rf /dev/shm/keywork
```

> Had je op de SSD gewerkt in plaats van in `/dev/shm`, dan is `shred` daar **niet** betrouwbaar — flash/SSD laat zich niet veilig per bestand overschrijven. Precies daarom de RAM-route.

Herstel — zodat je weet dat het werkt

Vanaf de kaart

```
sudo cryptsetup open /dev/sdX keybackup
sudo mount /dev/mapper/keybackup /mnt/keybackup
gpg --import /mnt/keybackup/PRIVE_VOLLEDIG.asc
```

Vanaf papier (als alle kaarten stuk zijn)

Je hebt de afdruk **plus** de publieke sleutel nodig:

```
paperkey --pubring PUBLIEK.asc --secrets masterkey-paperkey.txt \
         --output PRIVE_HERSTELD.asc
gpg --import PRIVE_HERSTELD.asc
```

> **Daarom ligt de publieke sleutel mee op de kaart:** zonder hem is het papieren anker nutteloos. Samen maken ze herstel mogelijk.

> **Samengevat.** f3-check → LUKS → sleutel + intrekkingscertificaat erop → paperkey afdrukken → in RAM werken en opruimen. **Twee kaarten op twee locaties, twee papieren afdrukken.** Dan is je offline hoofdsleutel echt robuust beveiligd.