GNU Privacy Guard

- Der Herr der Schlüsselringe - so geht GPG

Schlüssel erstellen

```
# gpg --gen-key
```

Fragen entsprechend beantworten

Bei zusätzlichen Mailadressen auch für diese eine User ID erstellen

```
# gpg --edit-key meine@Hauptmailadresse
```

```
gpg> adduid
```

... Fragen entsprechend beantworten (Hinweis: Kommentarfeld leer lassen!) und

zusätzliche@Mailadressse

als Mailadresse verwenden.

Erstellen eines "revocation certificate"

```
# gpg --gen-revoke meine@Hauptmailadresse > revoke.asc
```

Hinweis: mit einem hinreichend neuen GnuPG wird das revocation certificate automagisch erstellt und nach ~/.gnupg/openpgp-revocs.d/ gespeichert.

Öffentlichen Schlüssel exportieren

(XXXXXXX mit Deiner key ID ersetzen)

Öffentlichen Schlüssel lokal exportieren

```
# gpg --armor --output oldenburg.asc --export XXXX
```

Öffentlichen Schlüssel auf einen Keyserver hochladen

Den öffentlichen Schlüssel kannst Du dann noch auf einen Keyserver hochladen:

```
# gpg --list-keys  --with-colons meine@Hauptmailadresse | awk -F: '$1 == "pub" { print $5 }'
XXXXXXXX
# gpg --send-keys --keyserver hkps://keys.openpgp.org XXXXXX
```