Gnu Privacy Guard

“In der Praxis gibt es zwei Formen von Kryptographie: Mit der einen Form der Kryptographie können Sie Ihre Dateien vielleicht vor Ihrer kleinen Schwester schützen, mit der anderen Form vor dem Zugriff durch Organisationen der Regierung.”

Bruce Schneier, „Applied Cryptography“

- Was ist GnuPG?
- Wie funktioniert GnuPG?
  - Verschlüsselungskonzepte
  - Digitale Unterschriften
  - Digitale Zertifikate
- Demo

Was ist GnuPG?

- Verschlüsselung von Daten die nur vom Empfänger wieder entschlüsselt werden können
- Erzeugung einer Signatur über die versendeten Daten, um deren Authentizität und Integrität zu gewährleisten.
- GnuPG ist eine Weiterentwicklung aus PGP

Warum GnuPG?

Wie funktioniert GnuPG?

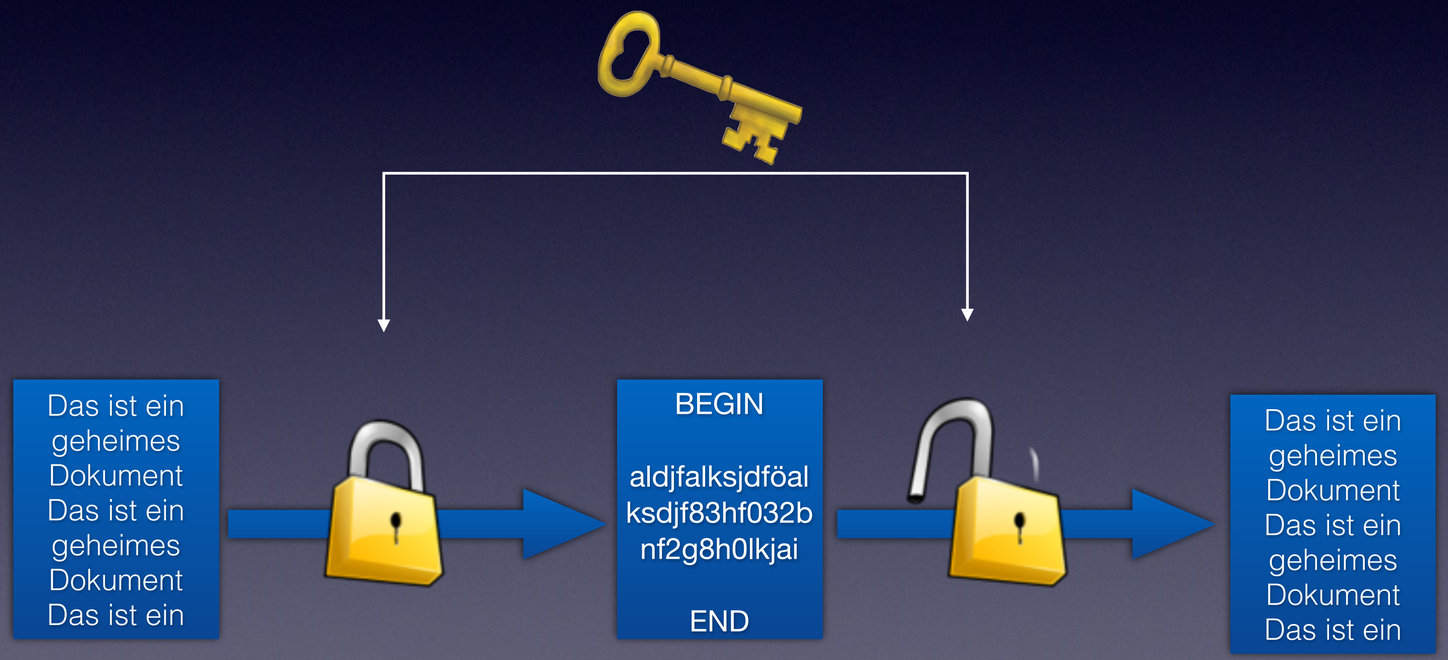
Wie funktioniert GnuPG?

Verschlüsselungskonzepte

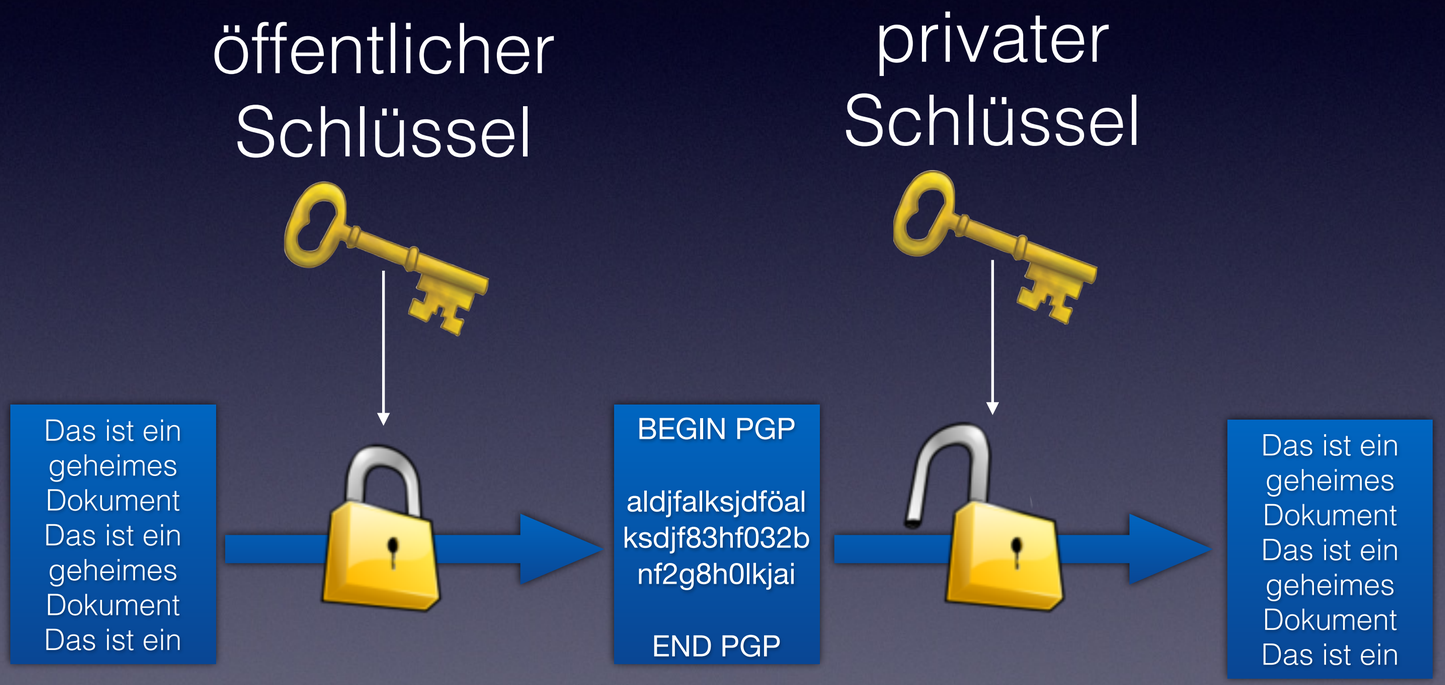
Verschlüsselungskonzepte

- Konventionelle Verschlüsselung (Symmetrisch)
- Public Key Verschlüsselung
- Hybride Verschlüsselung

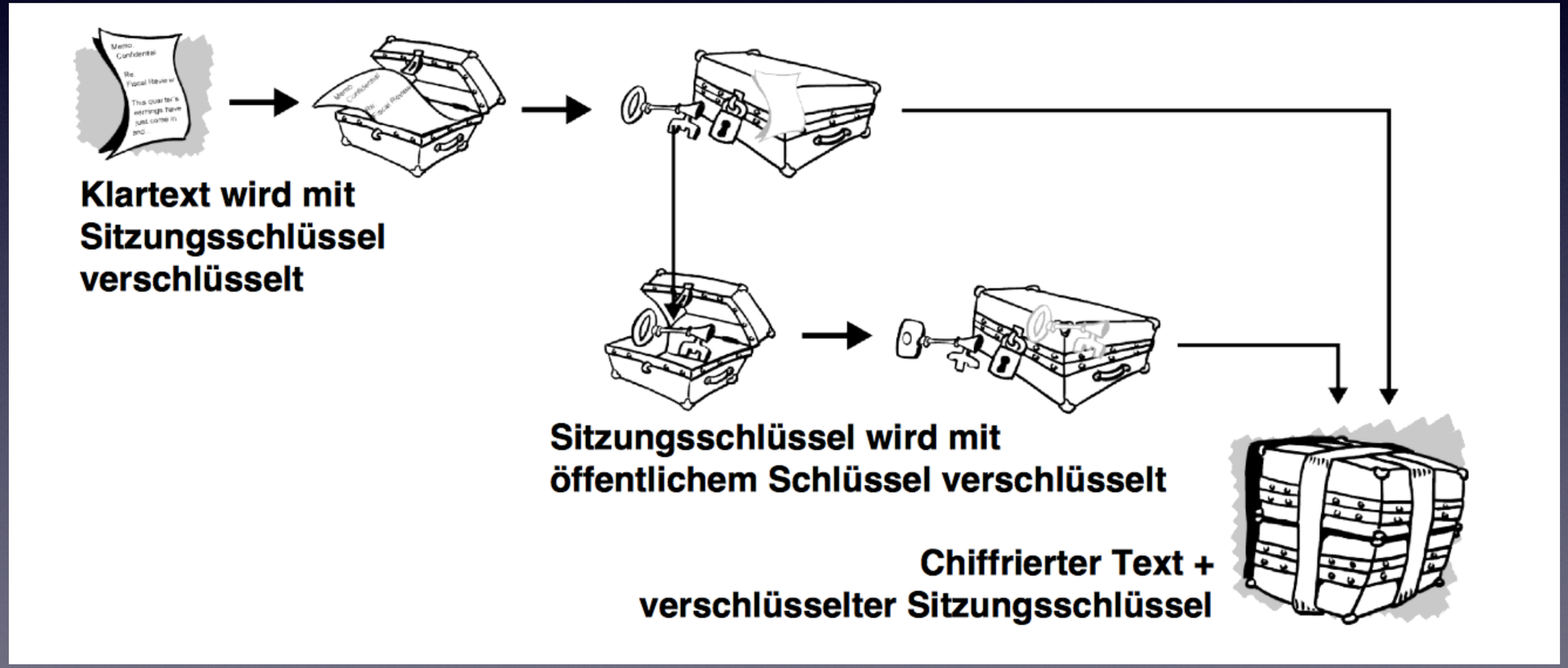
Konventionelle Verschlüsselung



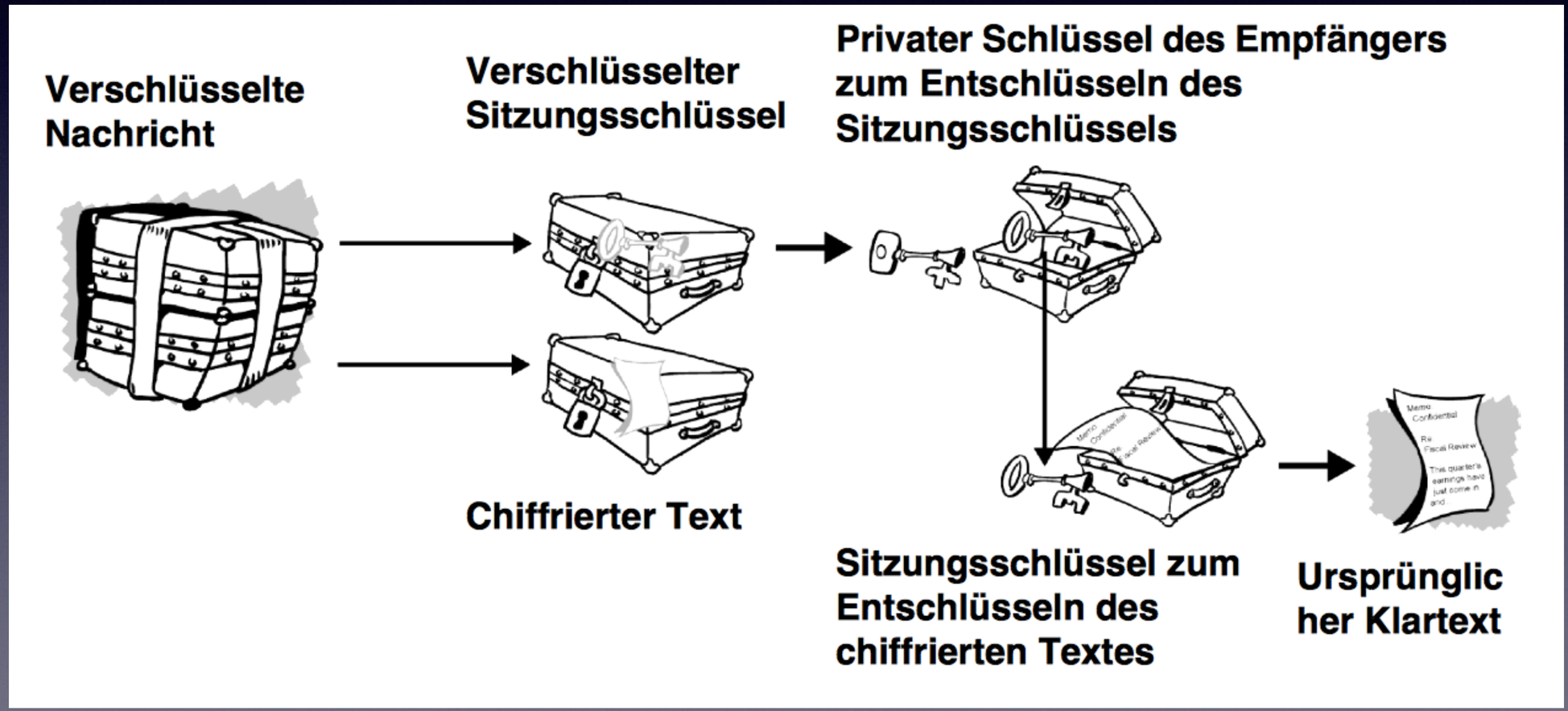
Public Key Verschlüsselung



Hybride Verschlüsselung



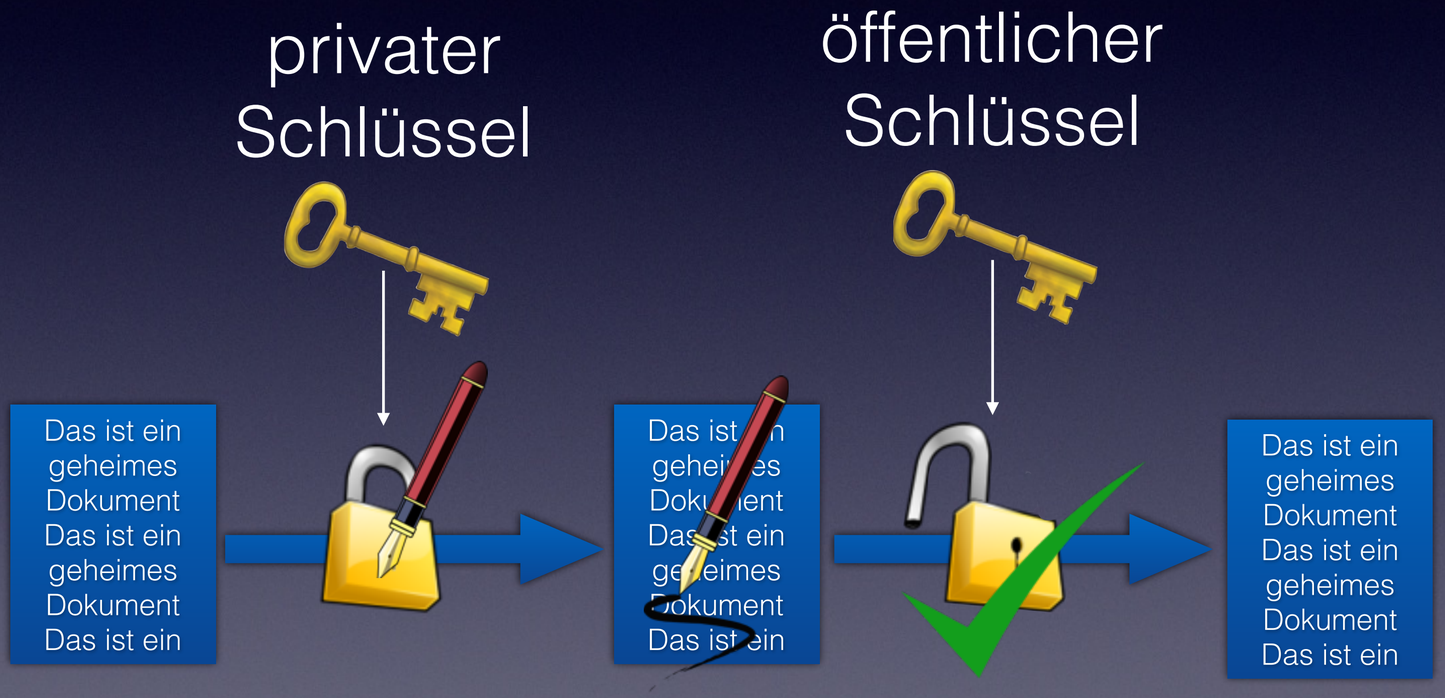
Hybride Verschlüsselung



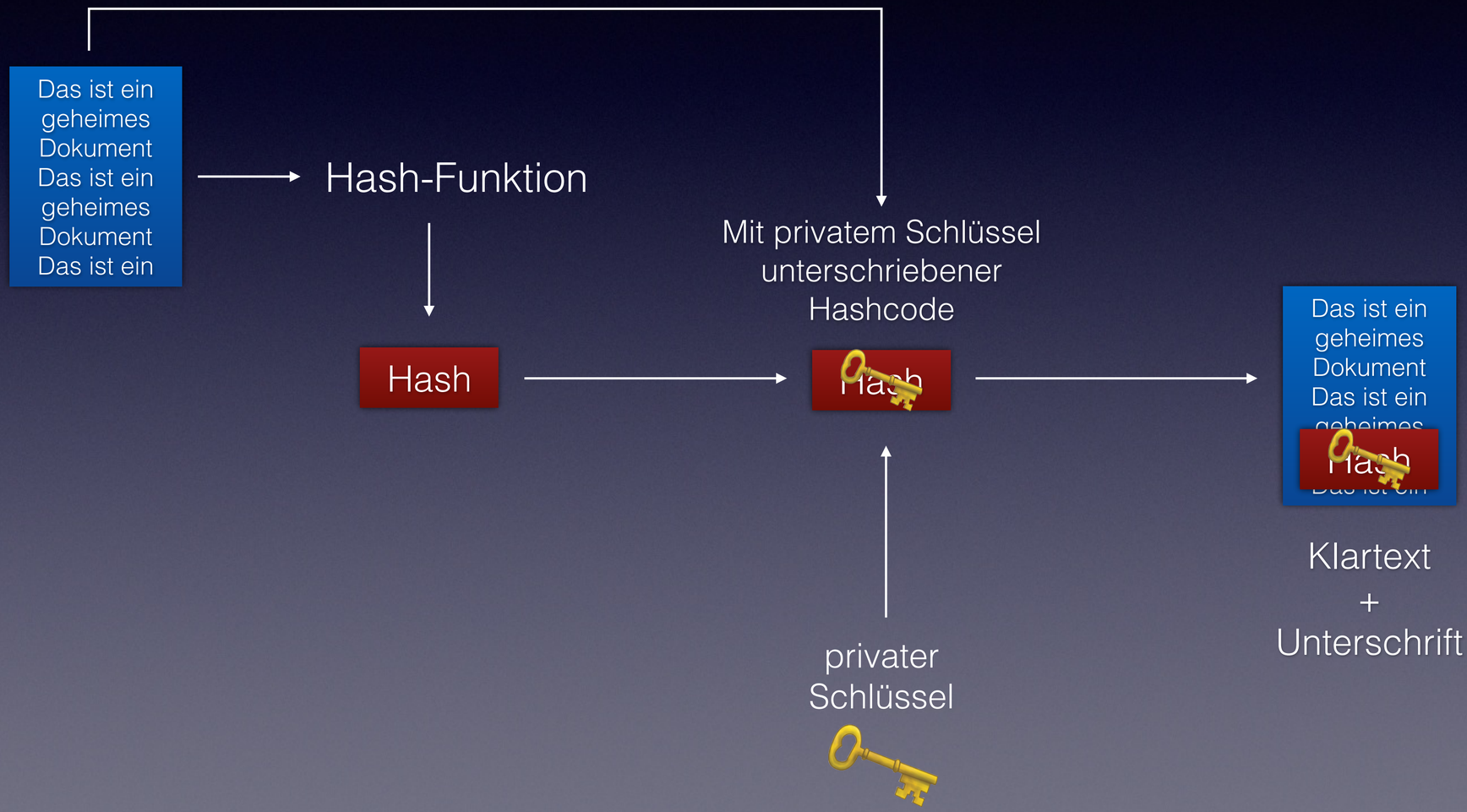
- Authentizität
- Integrität
- Nachweisbarkeit

Digitale Unterschriften

Digitale Unterschriften



Digitale Unterschriften



- Man kann nun Nachweisen, dass der Sender den Privatschlüssel zum öffentlichen Schlüssel hat

- die Echte Identität ist noch immer nicht bestätigt

Digitale Zertifikate

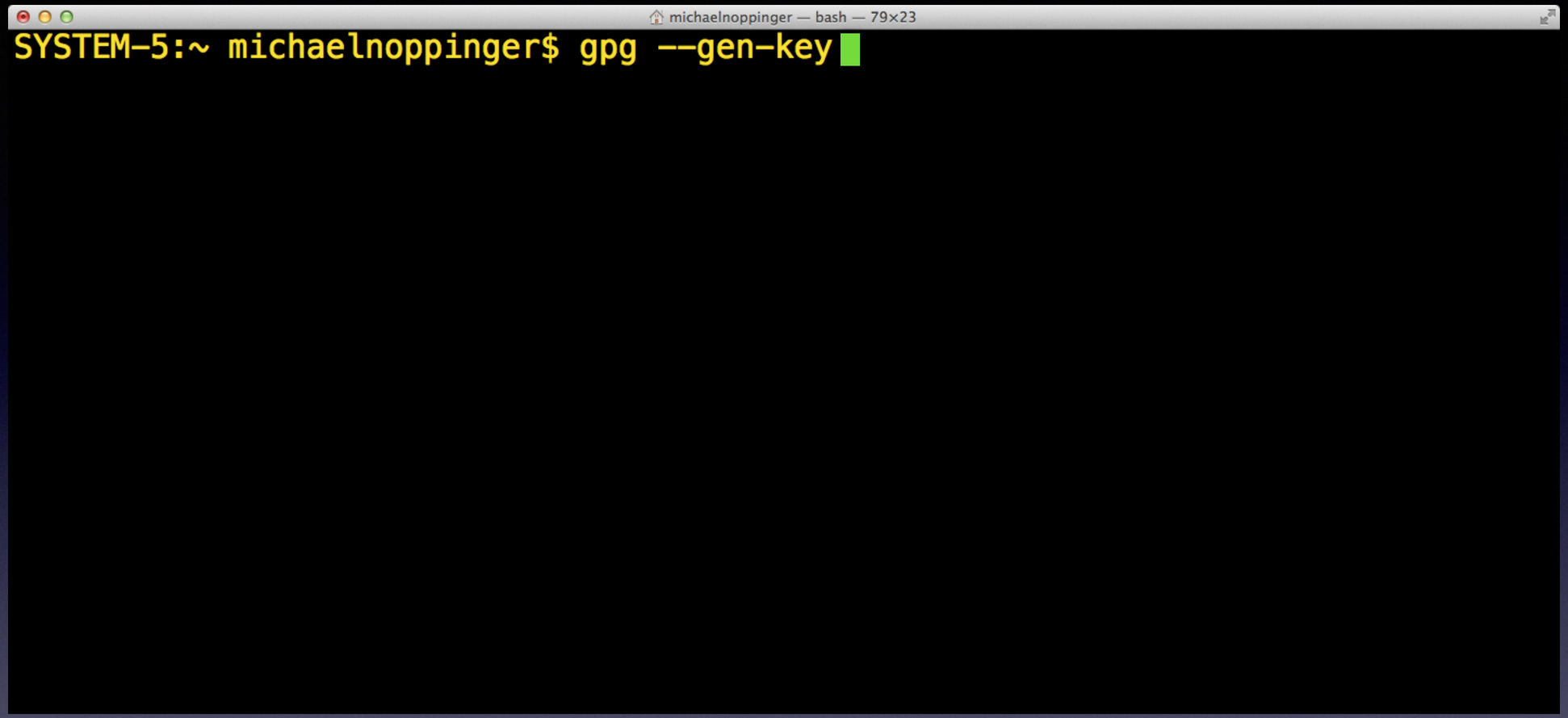
Digitale Zertifikate

- digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt
- Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten

Web of Trust

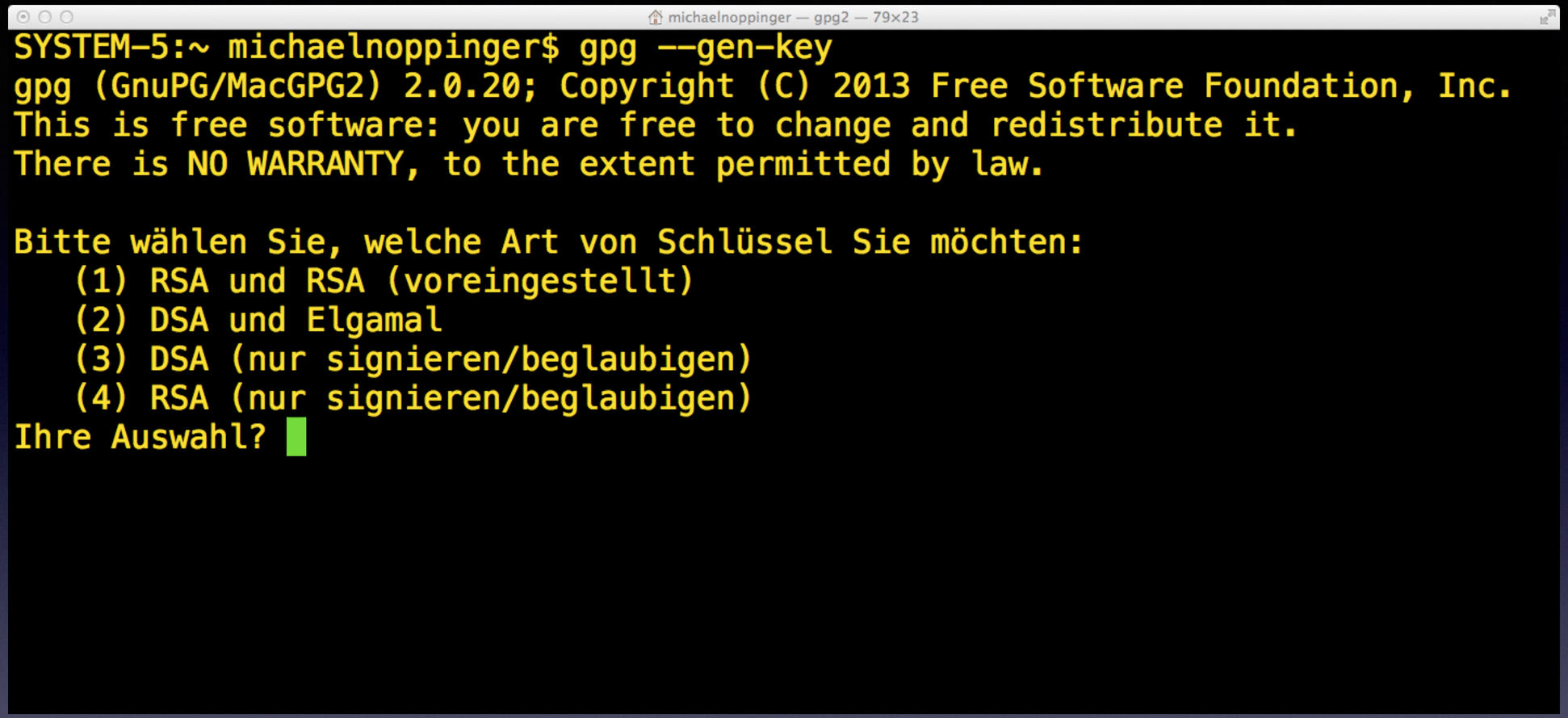
Demo

http://www.gnupg.org



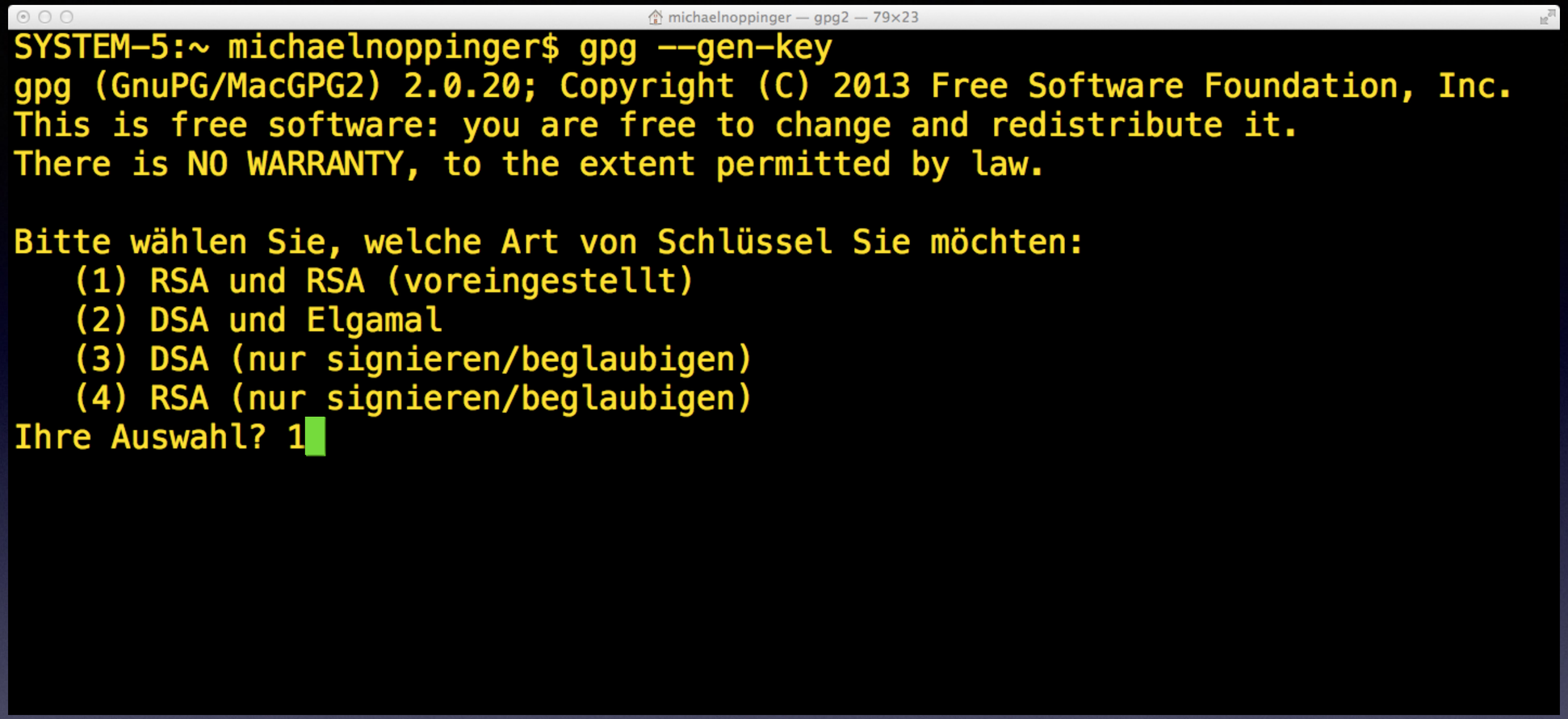
gpg --gen-key

Schlüssel erzeugen



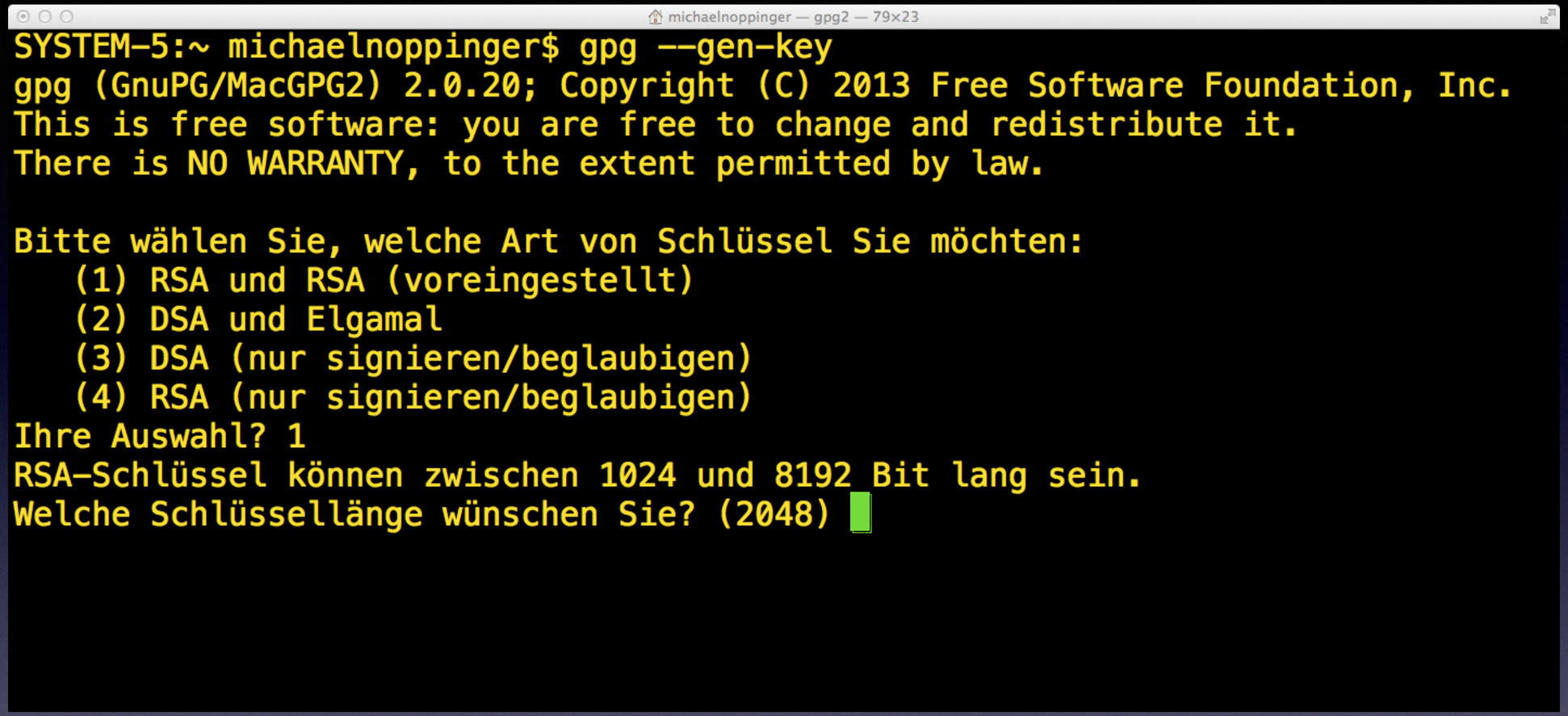
gpg --gen-key

Schlüssel erzeugen



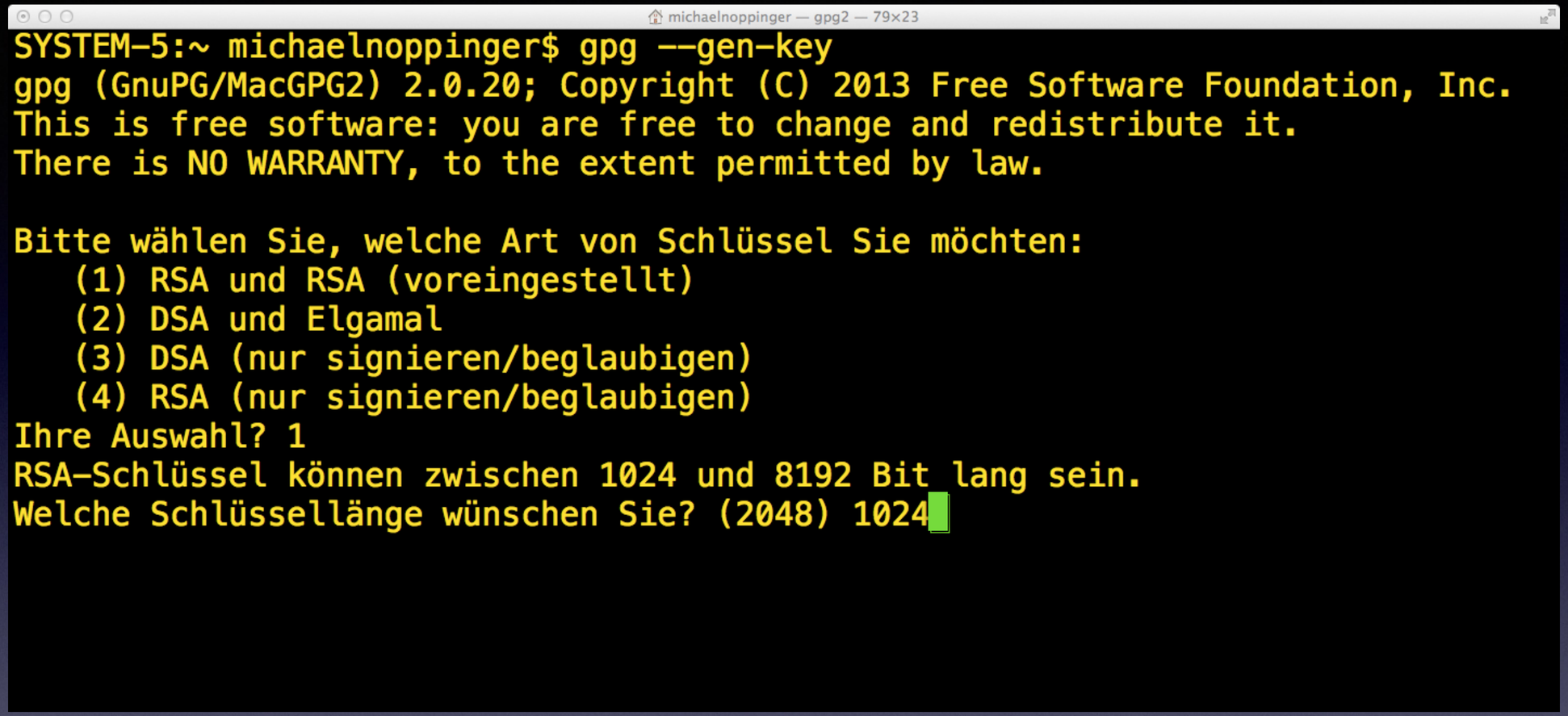
gpg --gen-key

Schlüssel erzeugen



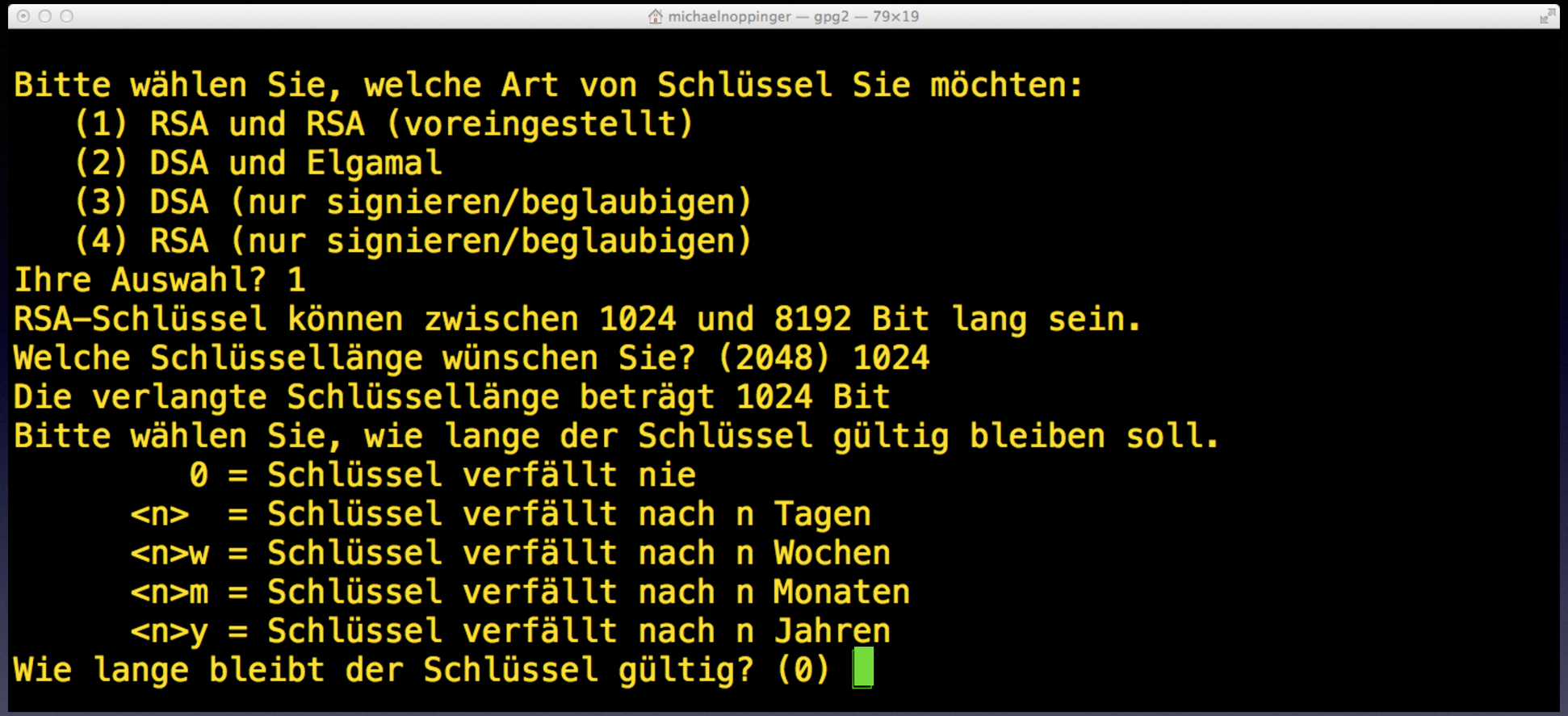
gpg --gen-key

Schlüssel erzeugen



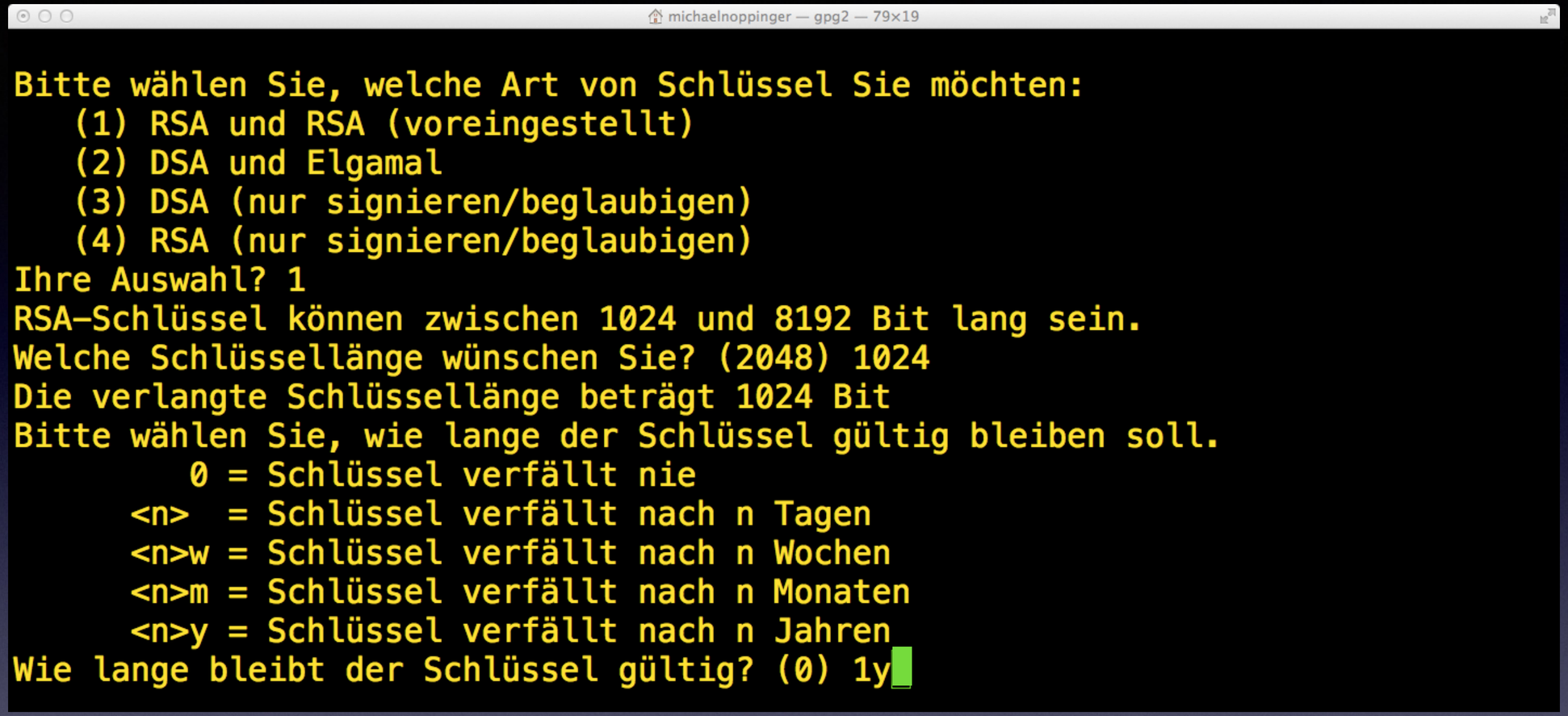
gpg --gen-key

Schlüssel erzeugen



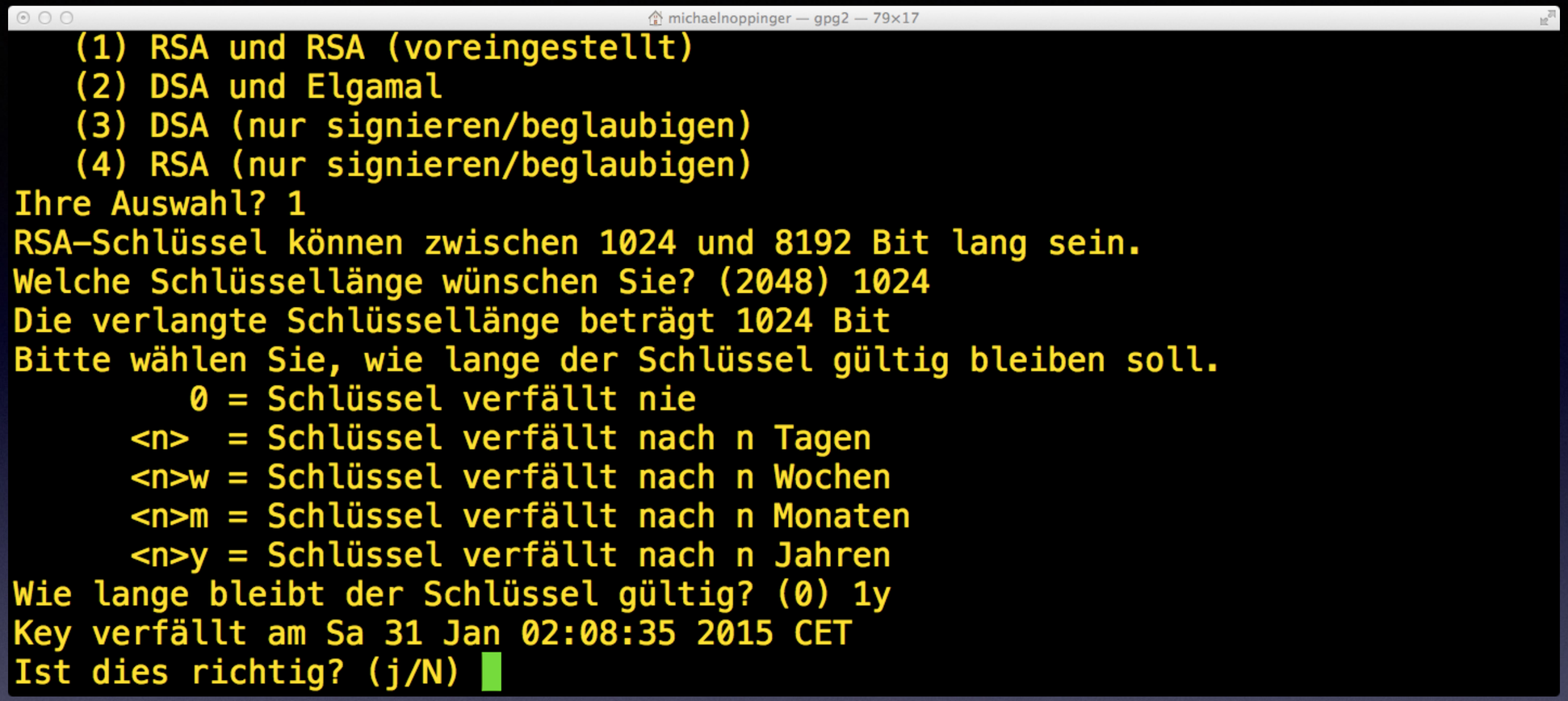
gpg --gen-key

Schlüssel erzeugen



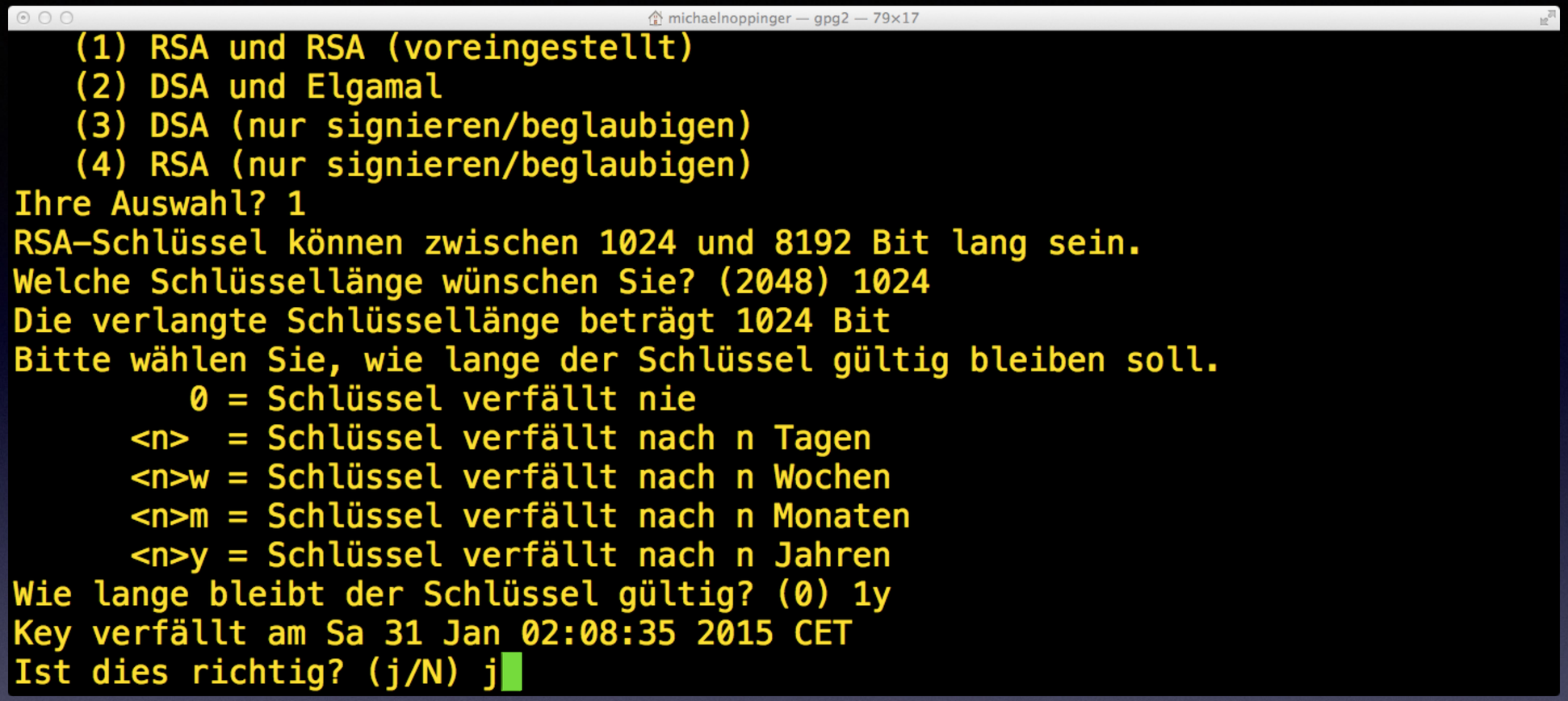
gpg --gen-key

Schlüssel erzeugen



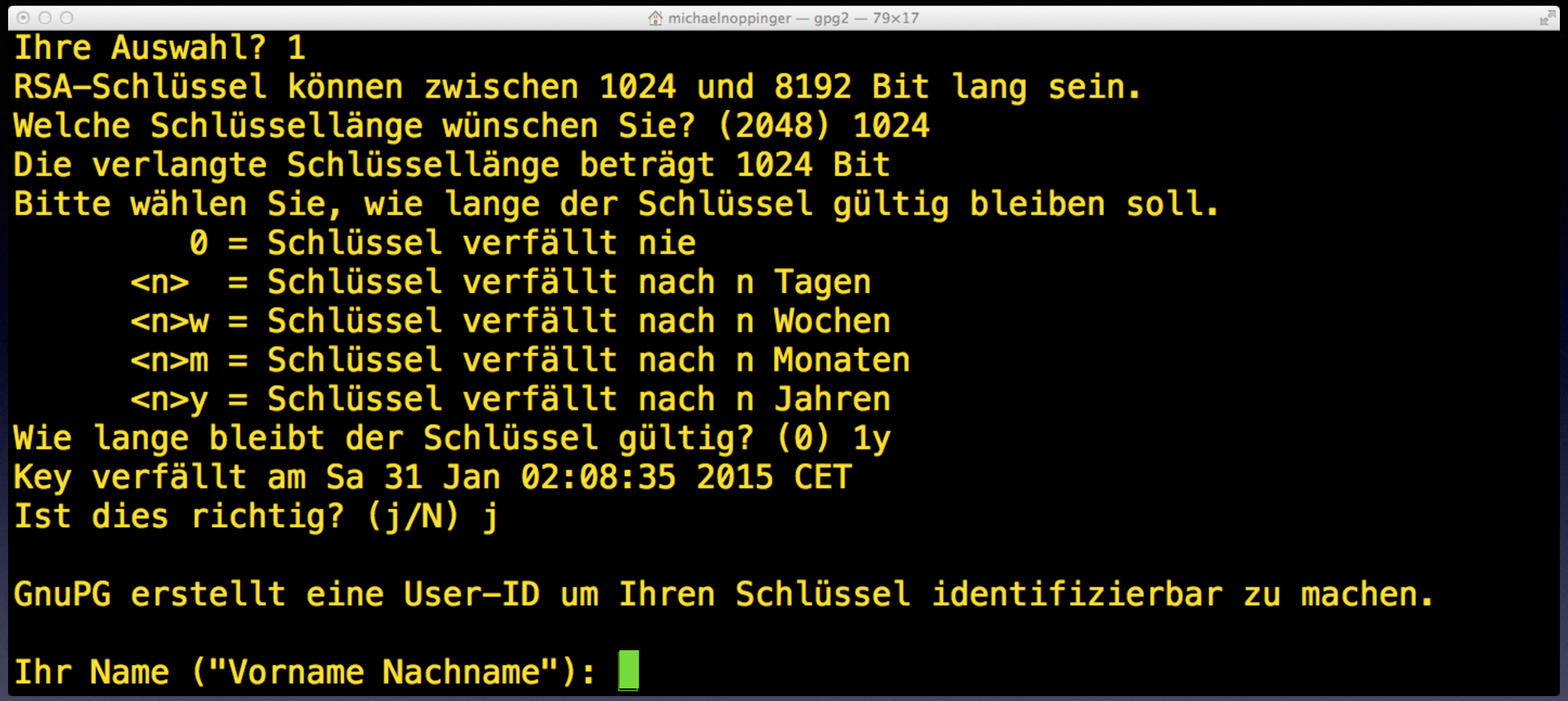
gpg --gen-key

Schlüssel erzeugen



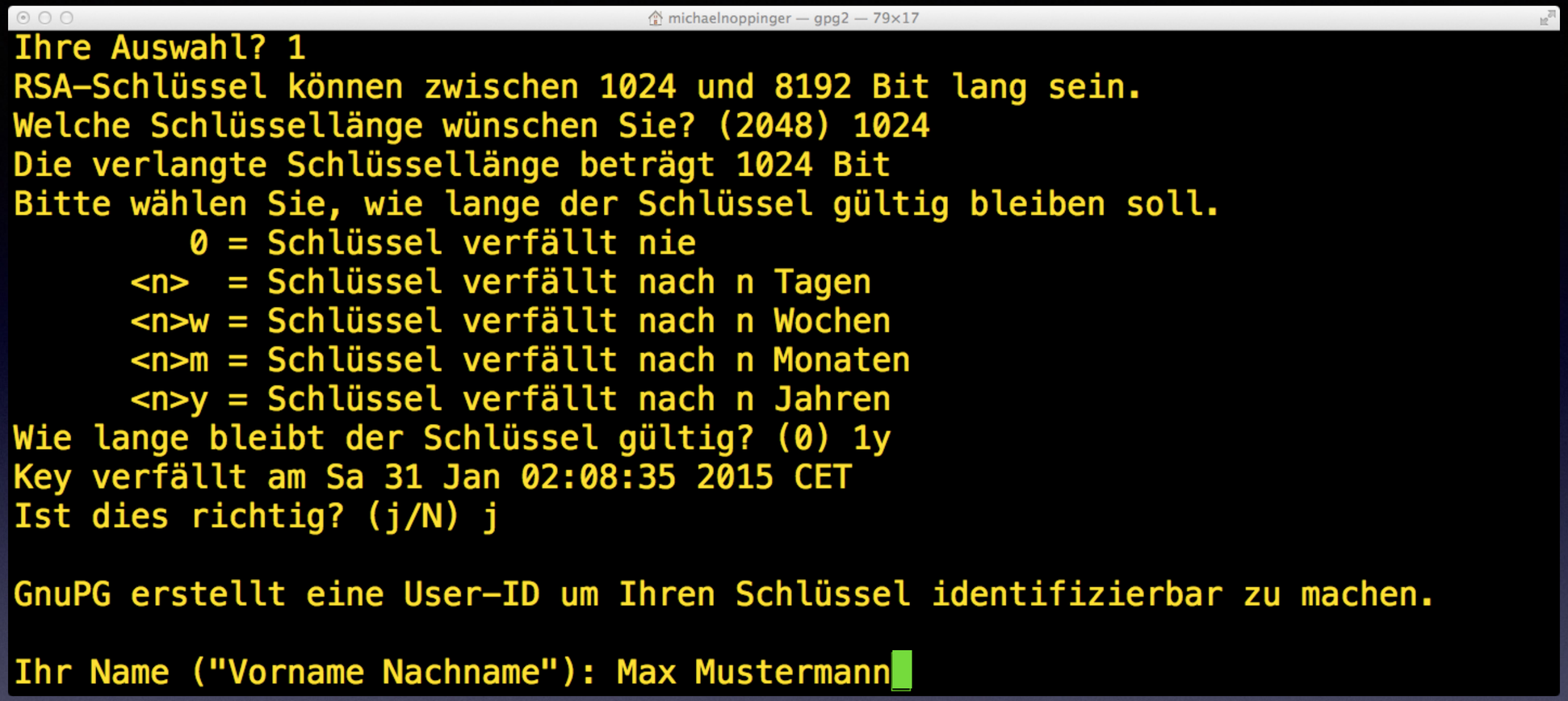
gpg --gen-key

Schlüssel erzeugen



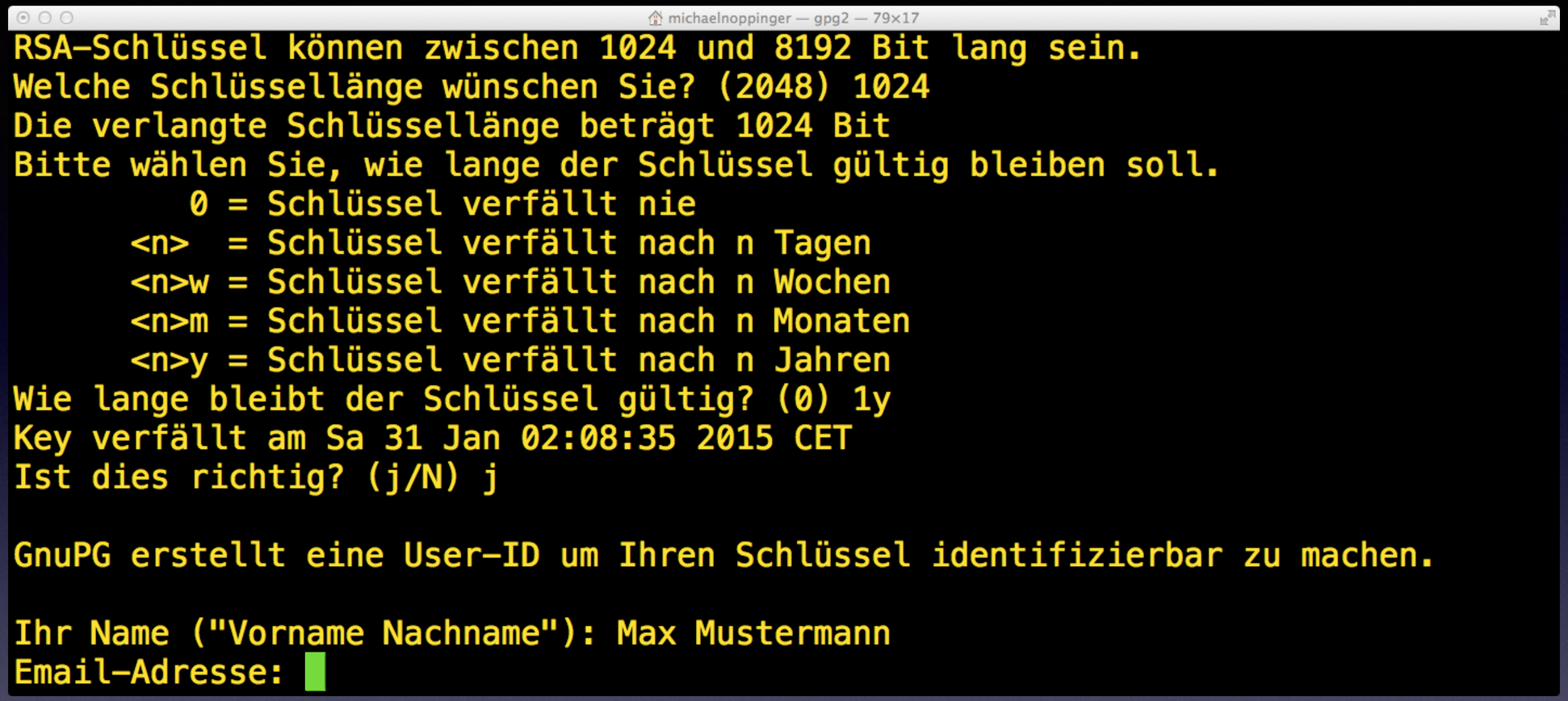
gpg --gen-key

Schlüssel erzeugen



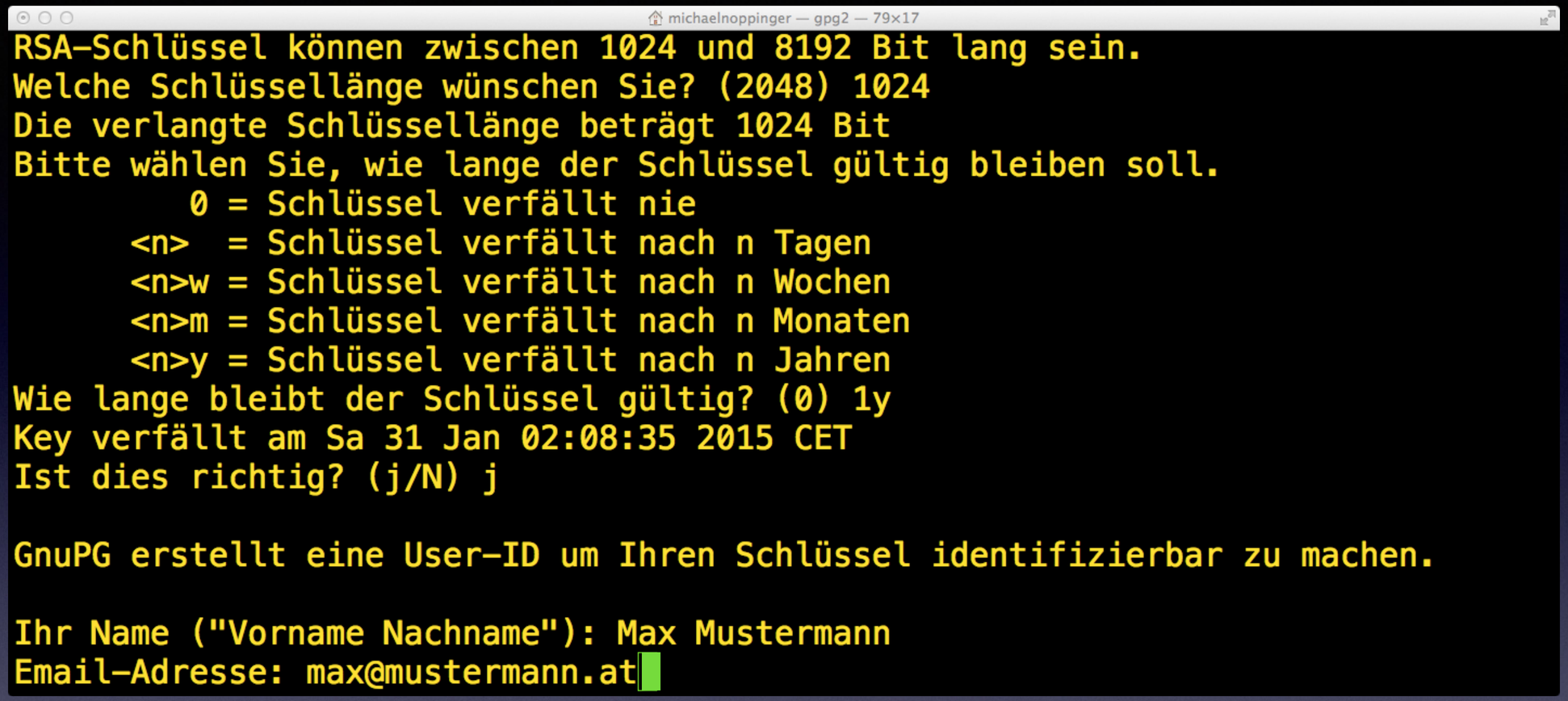
gpg --gen-key

Schlüssel erzeugen



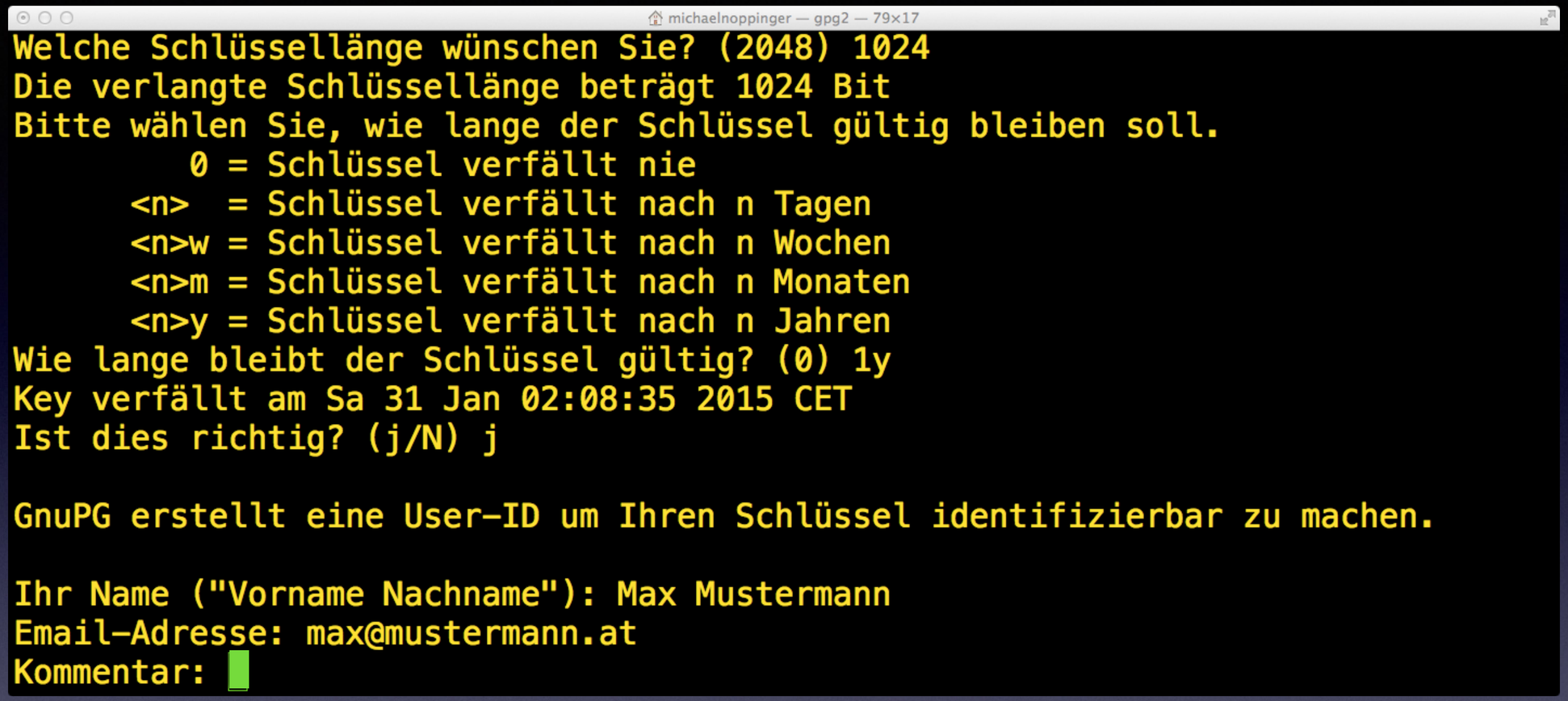
gpg --gen-key

Schlüssel erzeugen



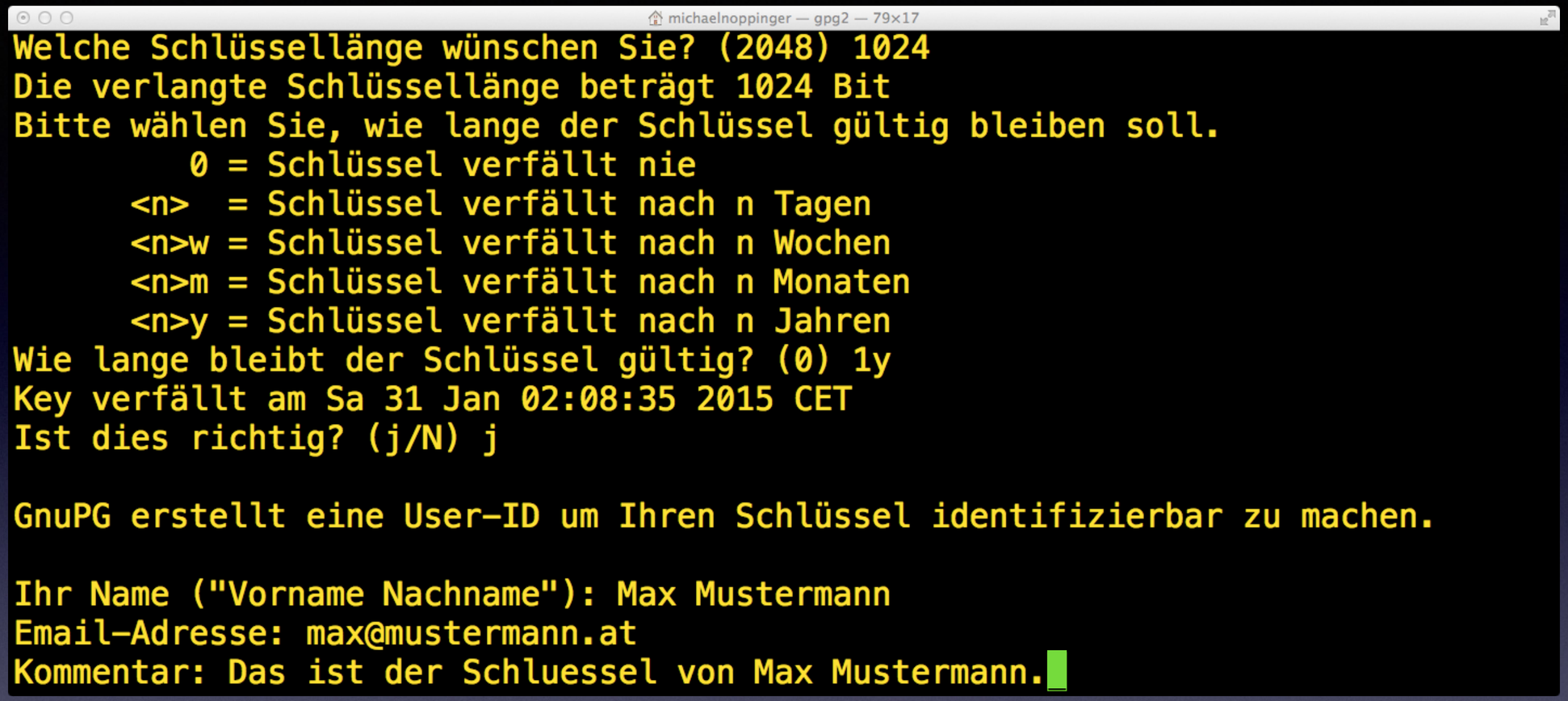
gpg --gen-key

Schlüssel erzeugen



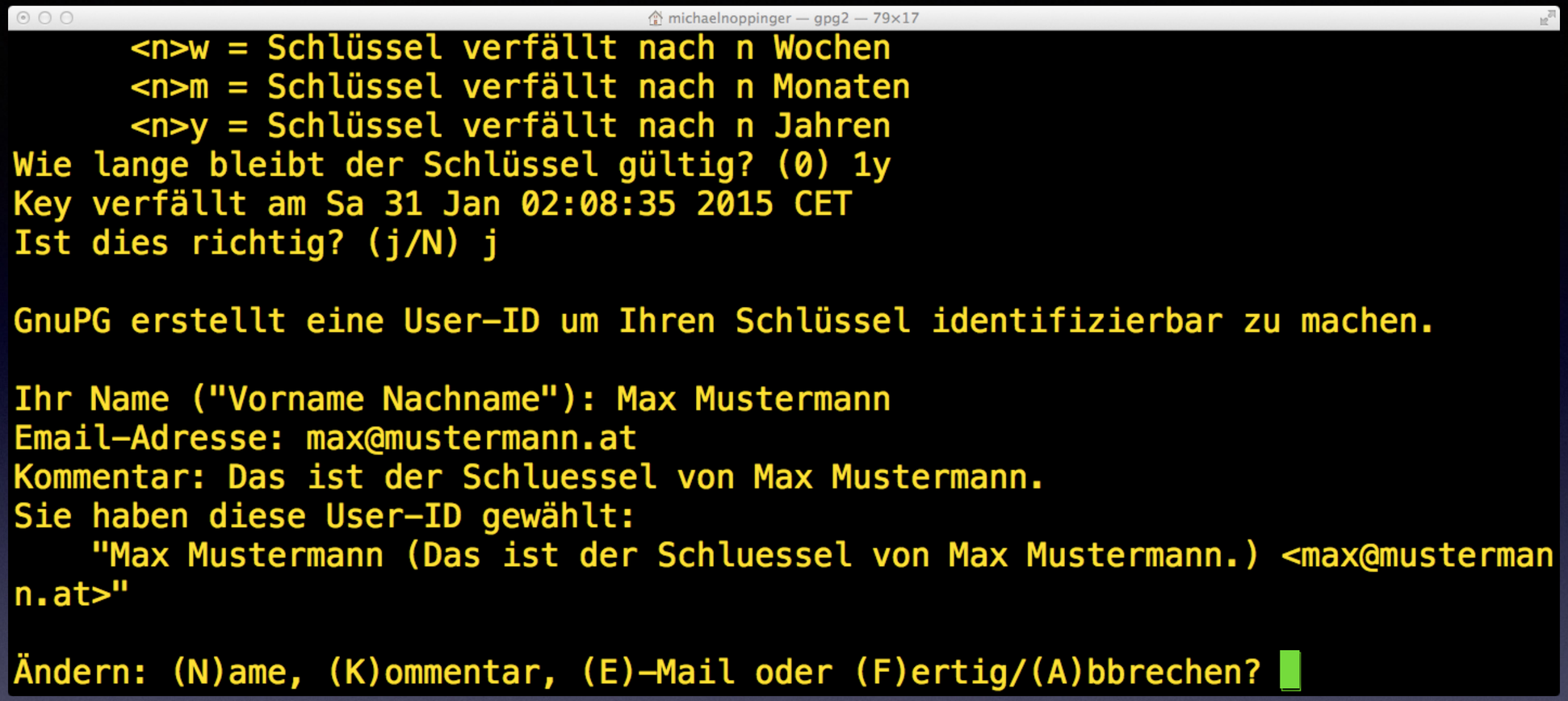
gpg --gen-key

Schlüssel erzeugen



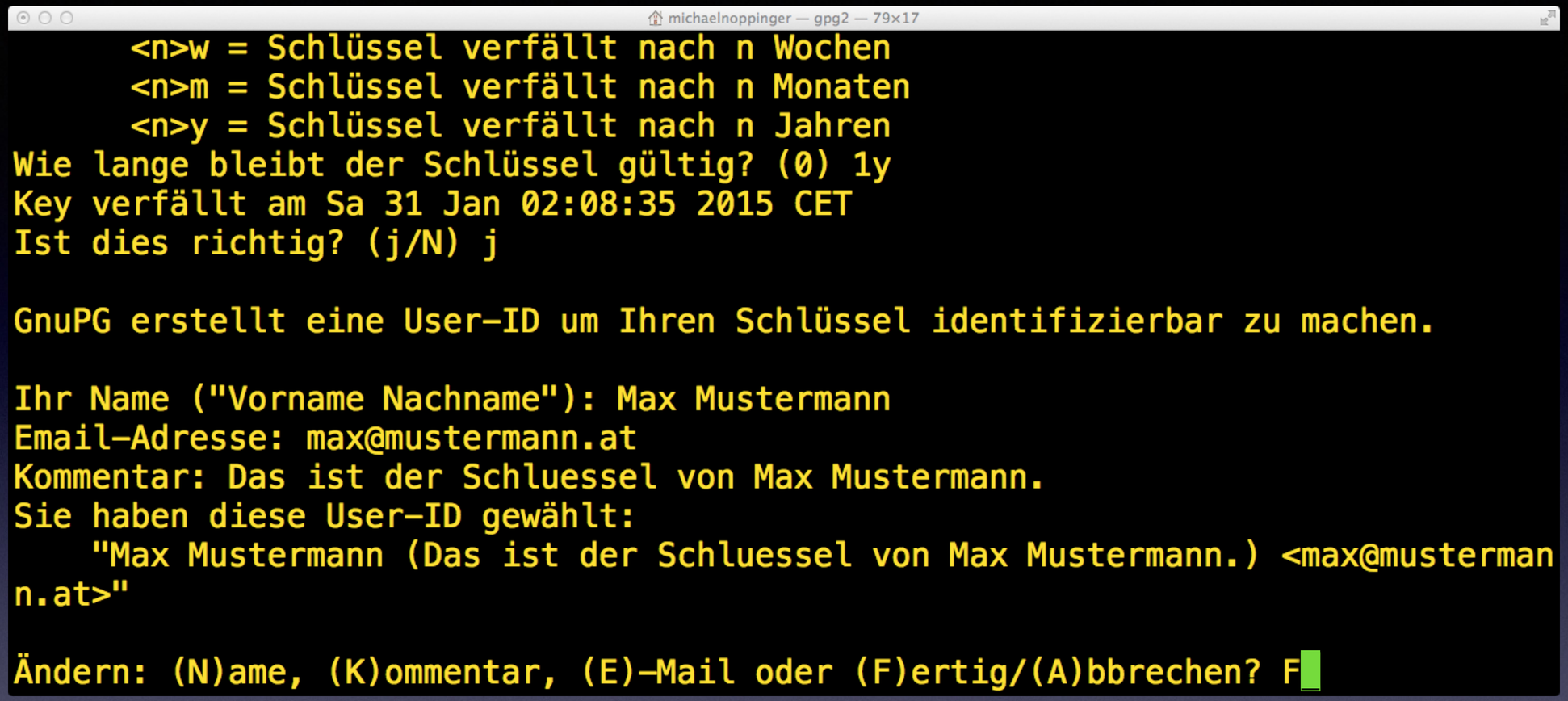
gpg --gen-key

Schlüssel erzeugen



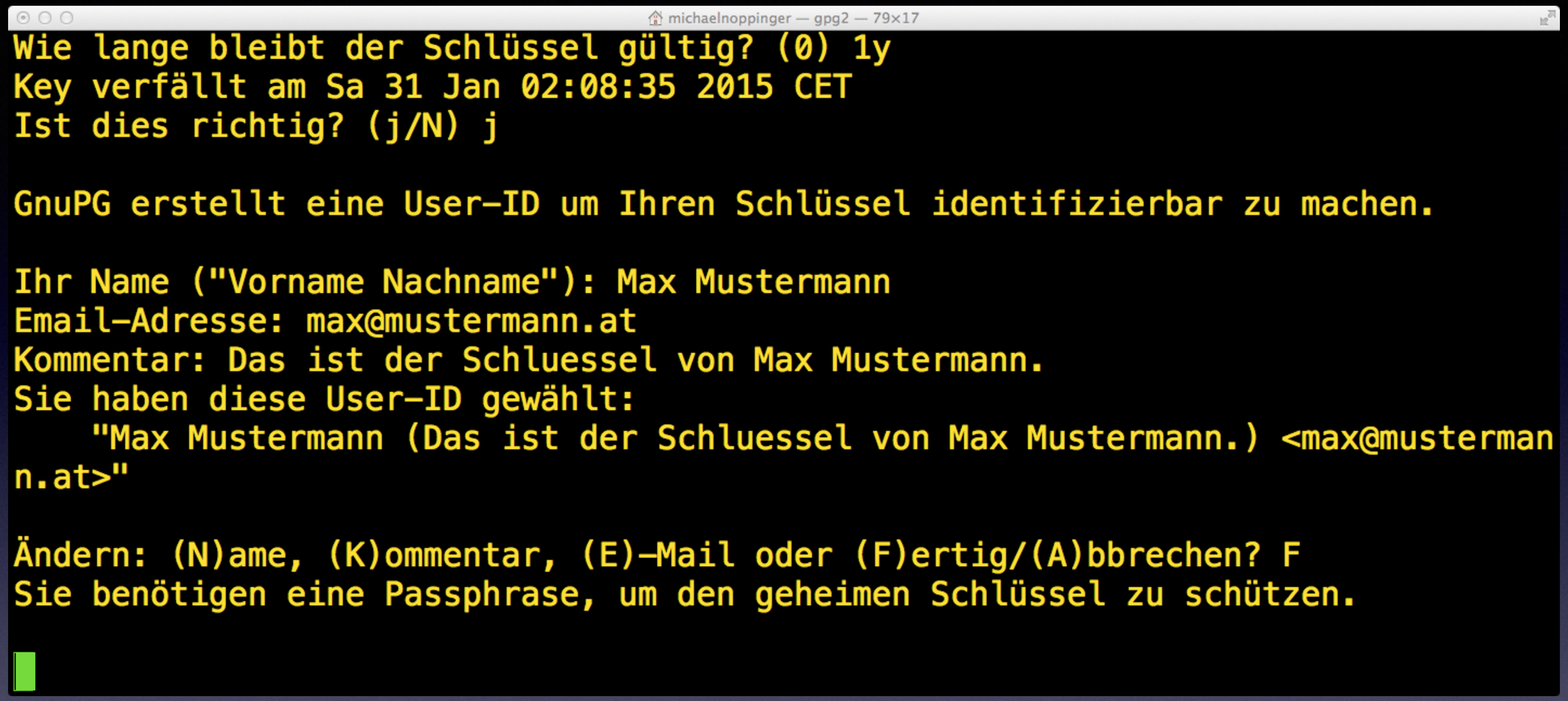
gpg --gen-key

Schlüssel erzeugen



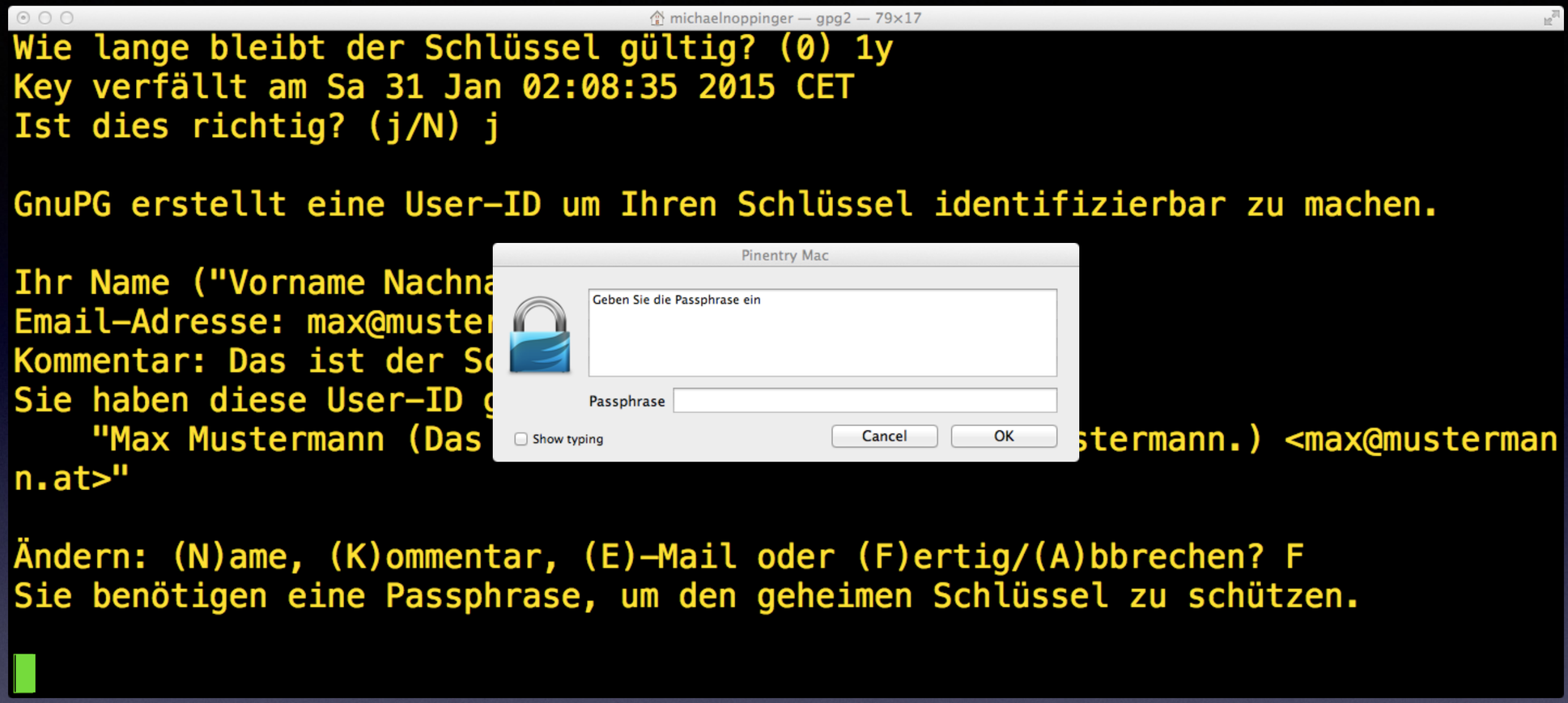
gpg --gen-key

Schlüssel erzeugen



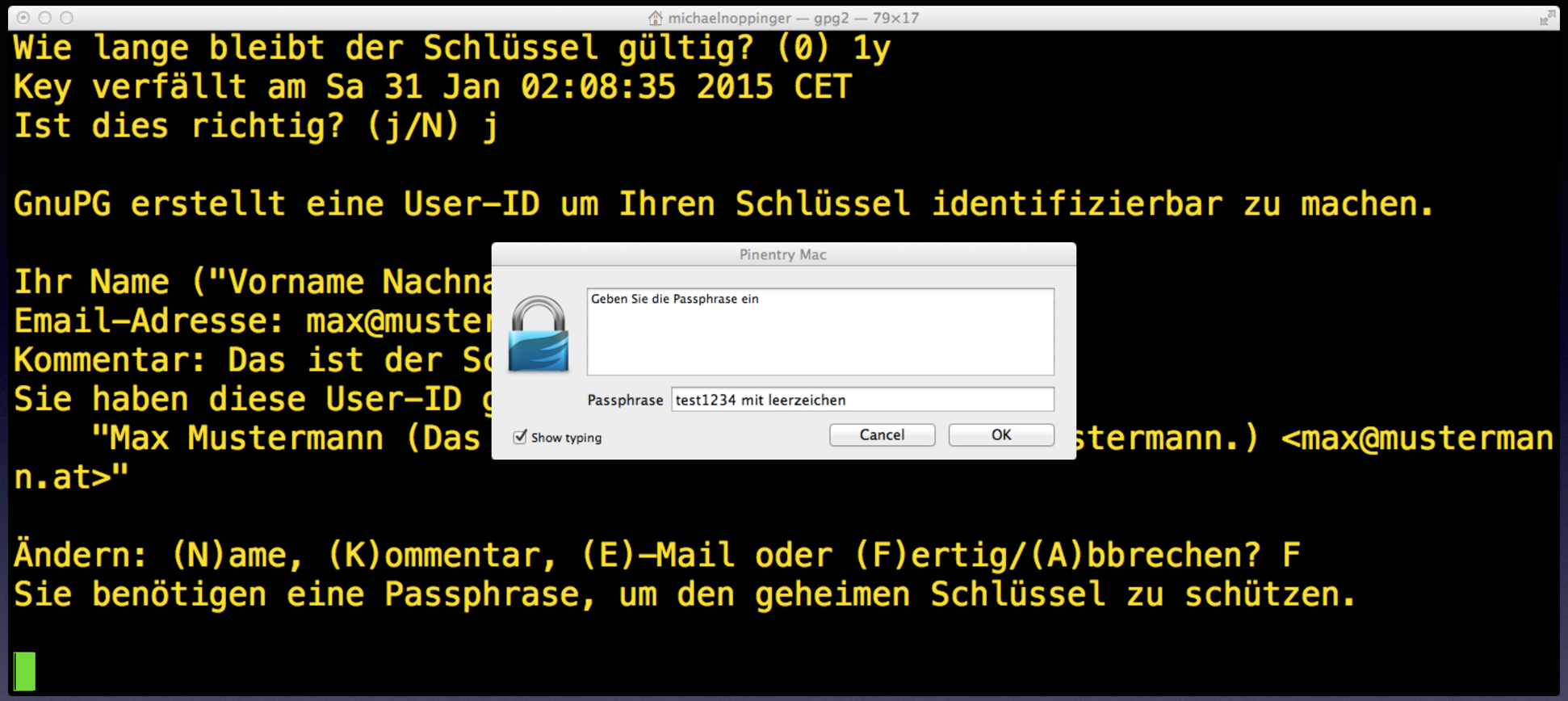
gpg --gen-key

Schlüssel erzeugen



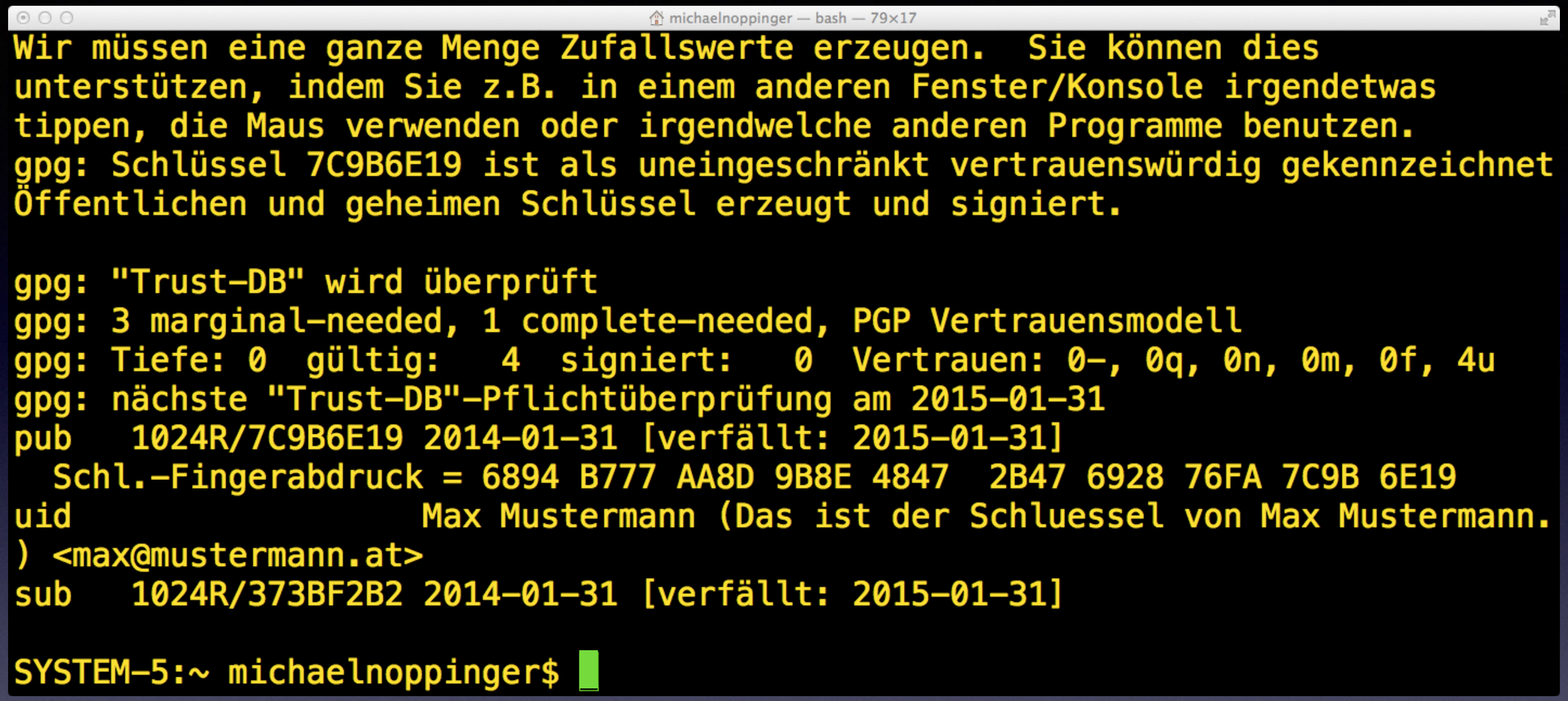
gpg --gen-key

Schlüssel erzeugen



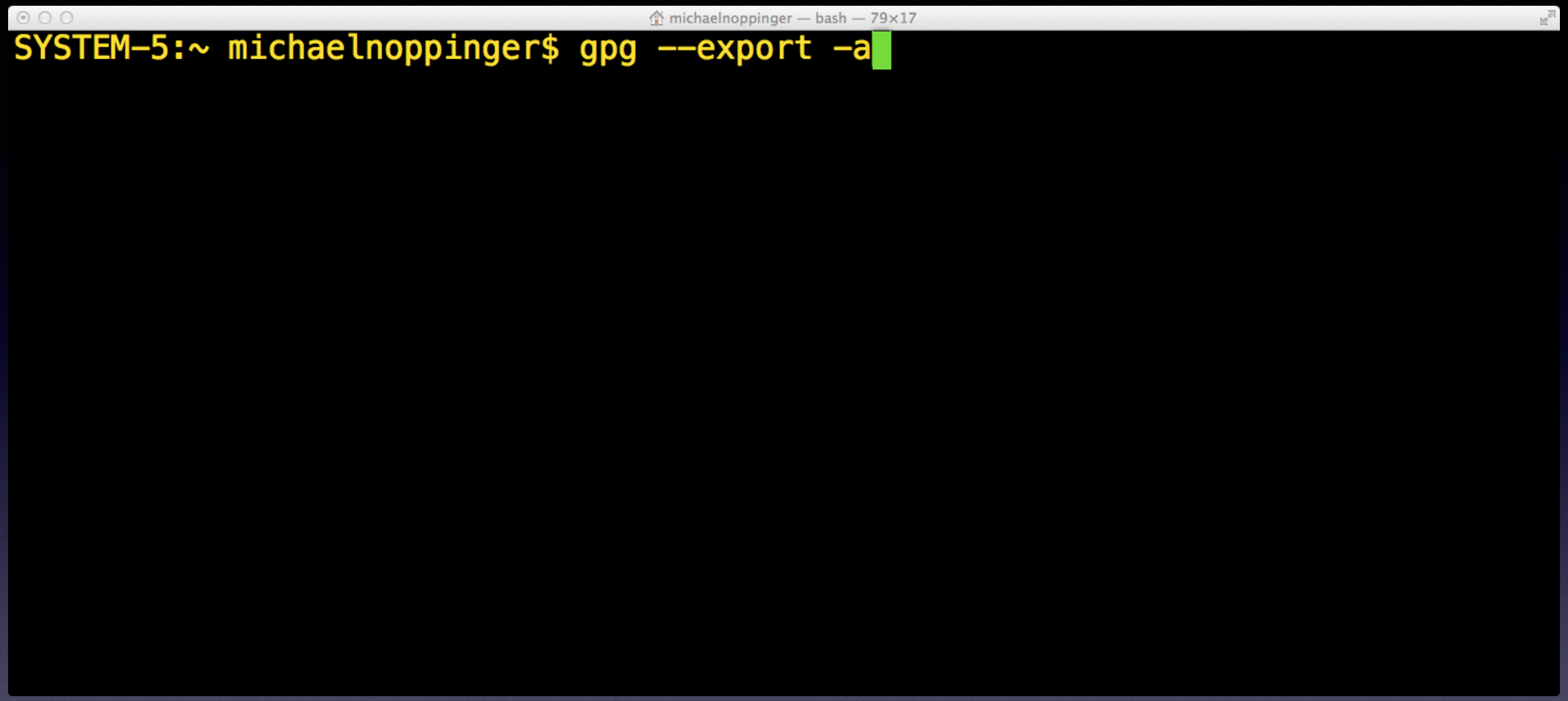
gpg --gen-key

Schlüssel erzeugen



gpg --gen-key

Schlüssel erzeugen



gpg –export [uid]

Schlüssel exportieren

gpg –export [uid]

Schlüssel exportieren

gpg –export [uid]

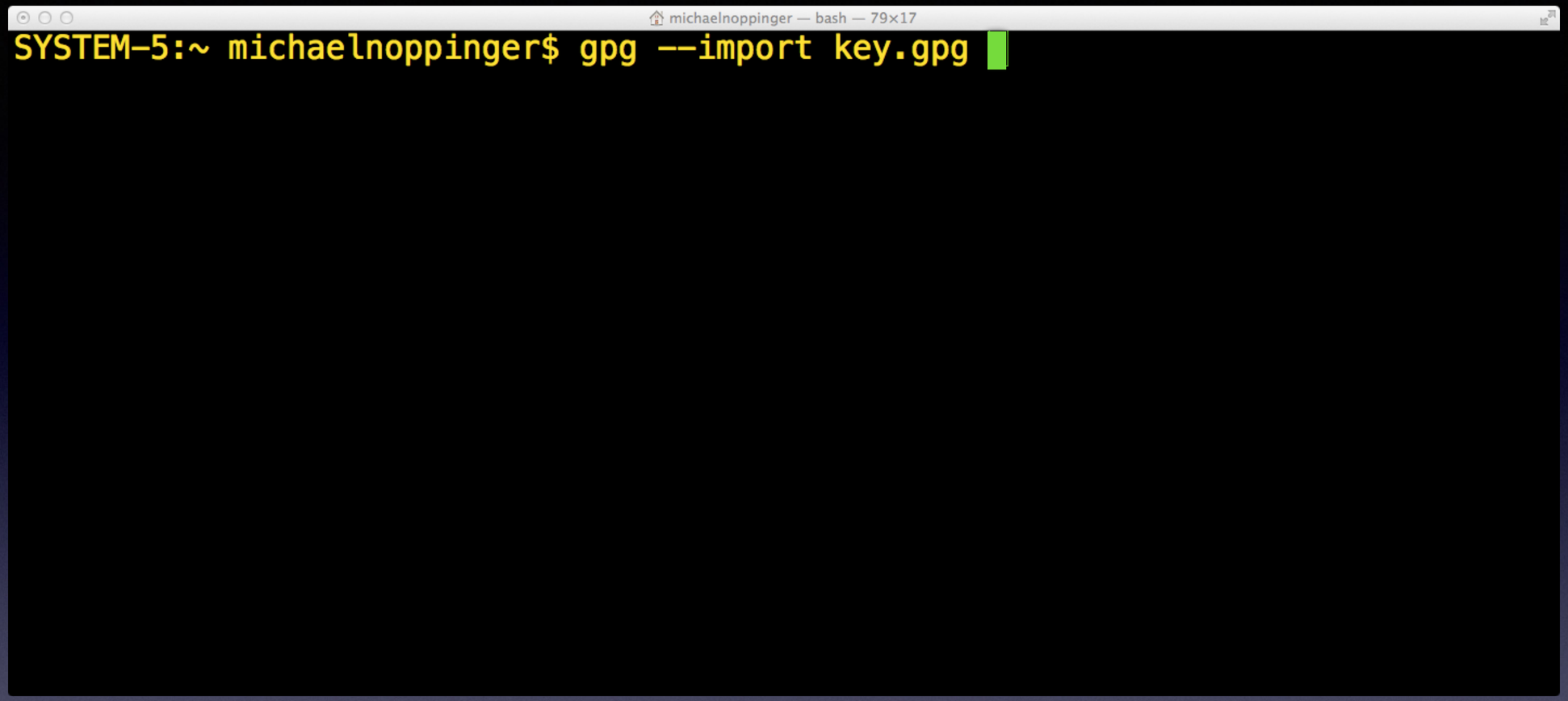
Schlüssel exportieren

gpg –export [uid]

Schlüssel exportieren

gpg –export [uid]

Schlüssel exportieren

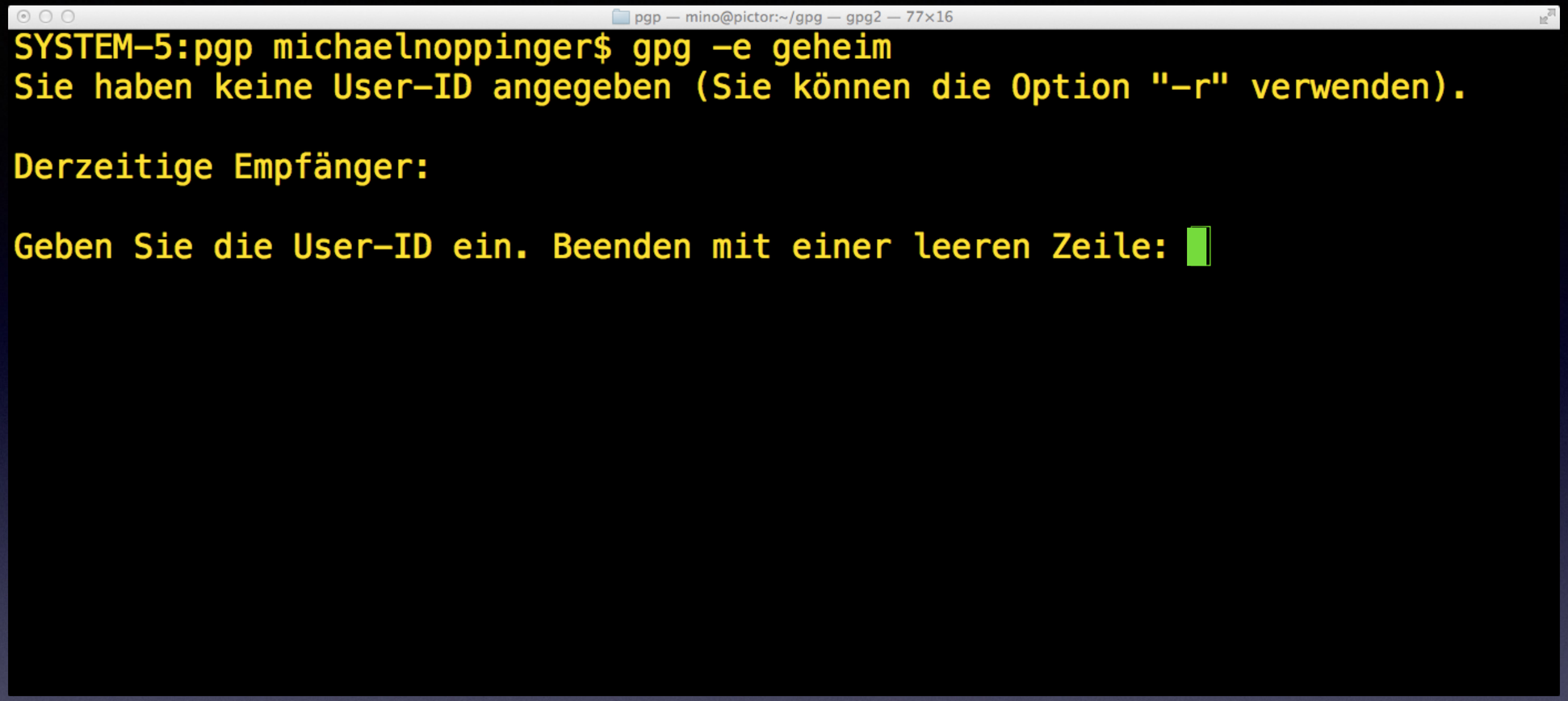


gpg –import [Datei]

Schlüssel importieren

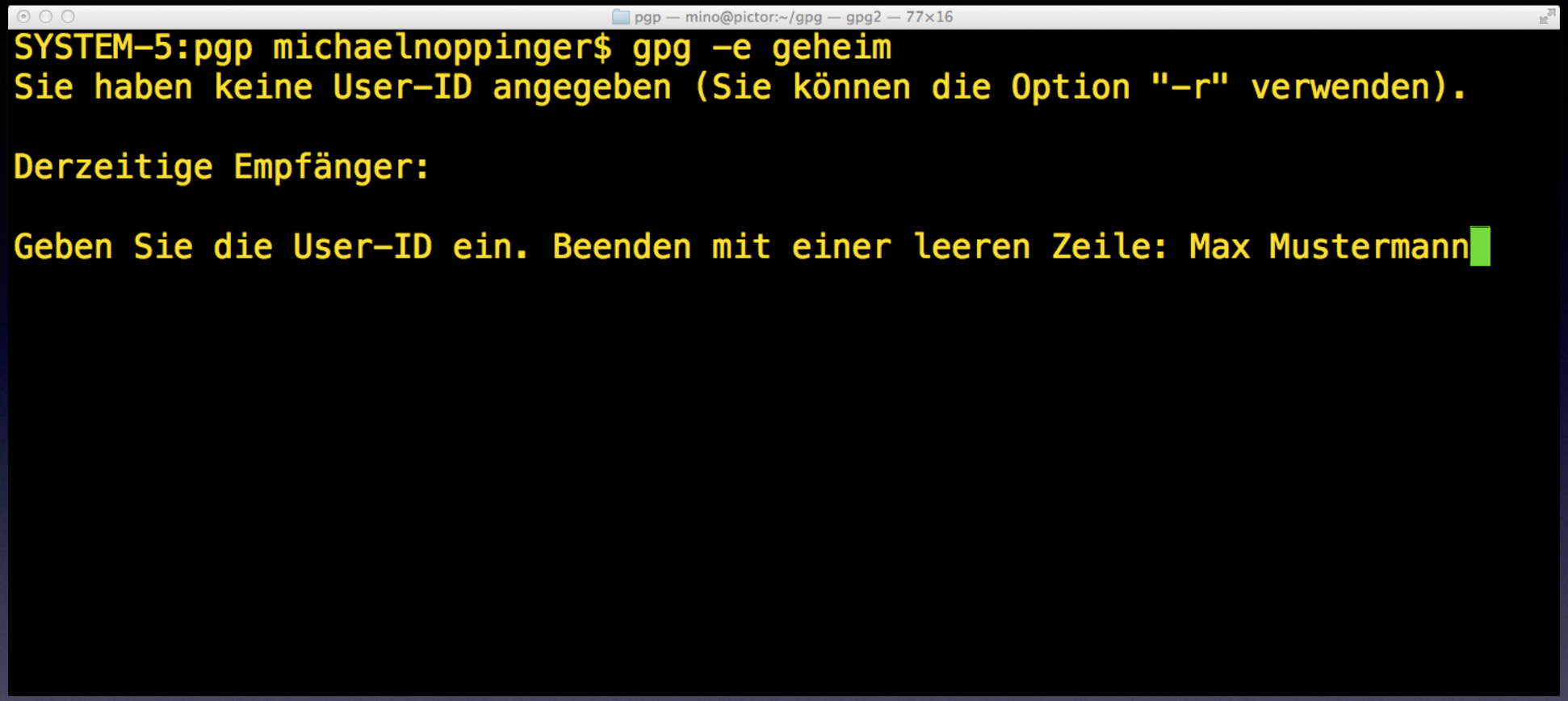
gpg -e[Datei] Empfänger

Verschlüsseln



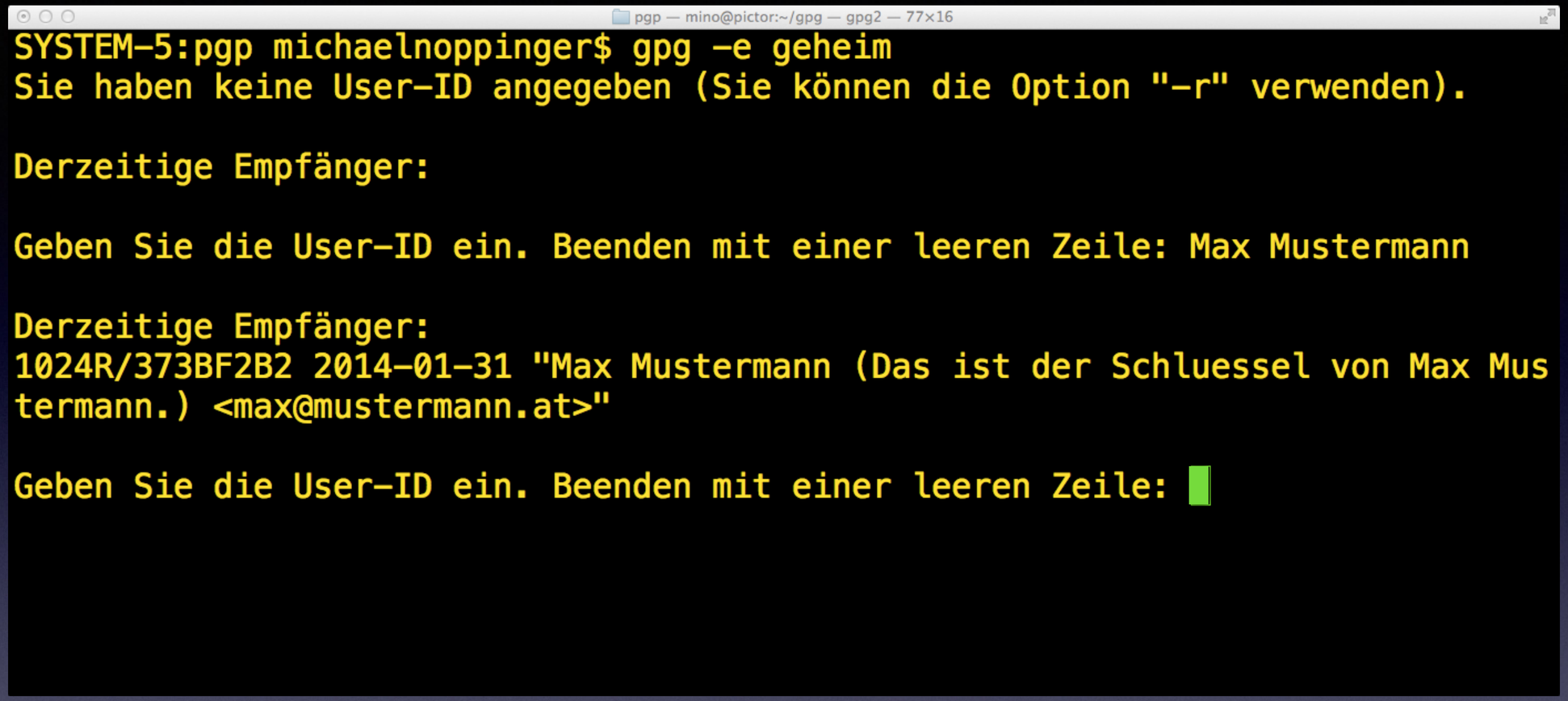
gpg -e[Datei] Empfänger

Verschlüsseln



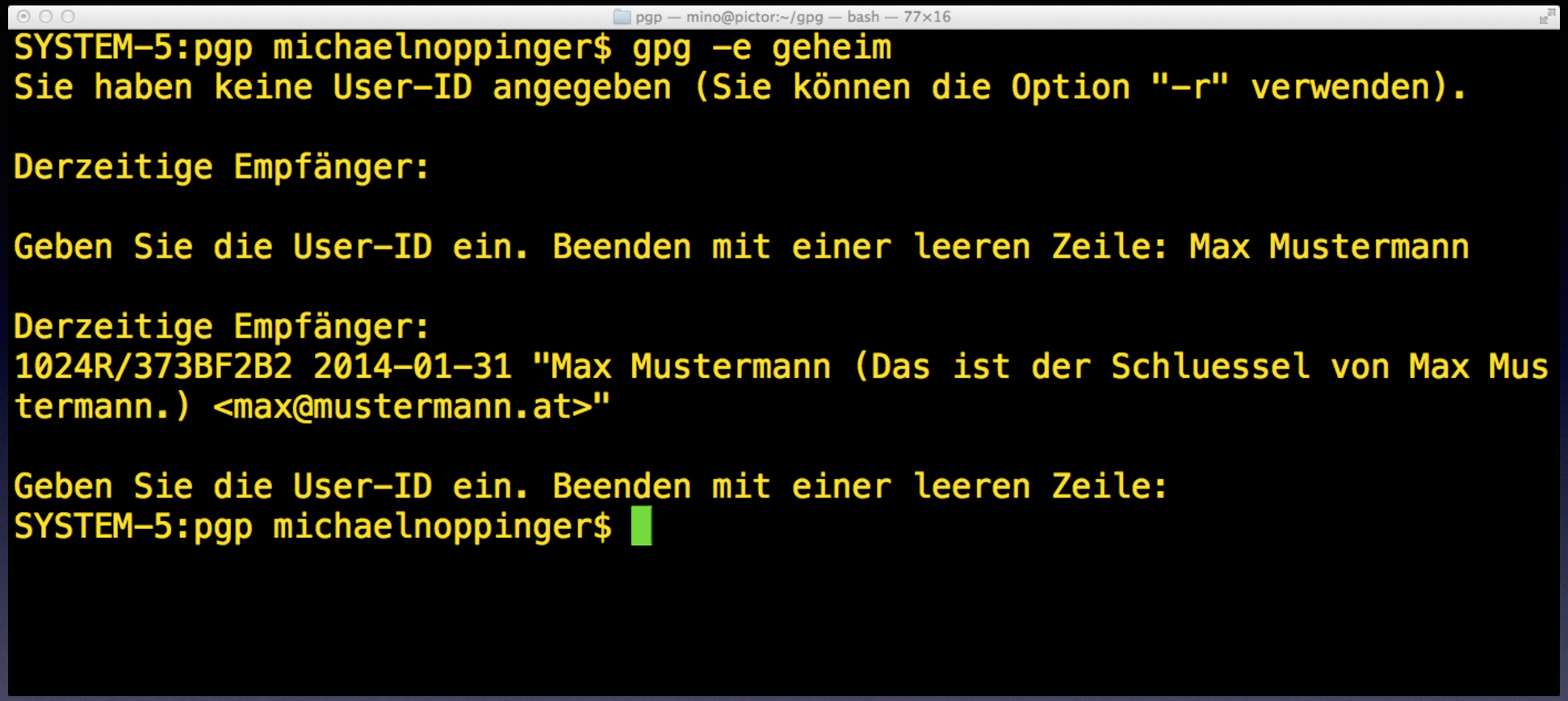
gpg -e[Datei] Empfänger

Verschlüsseln



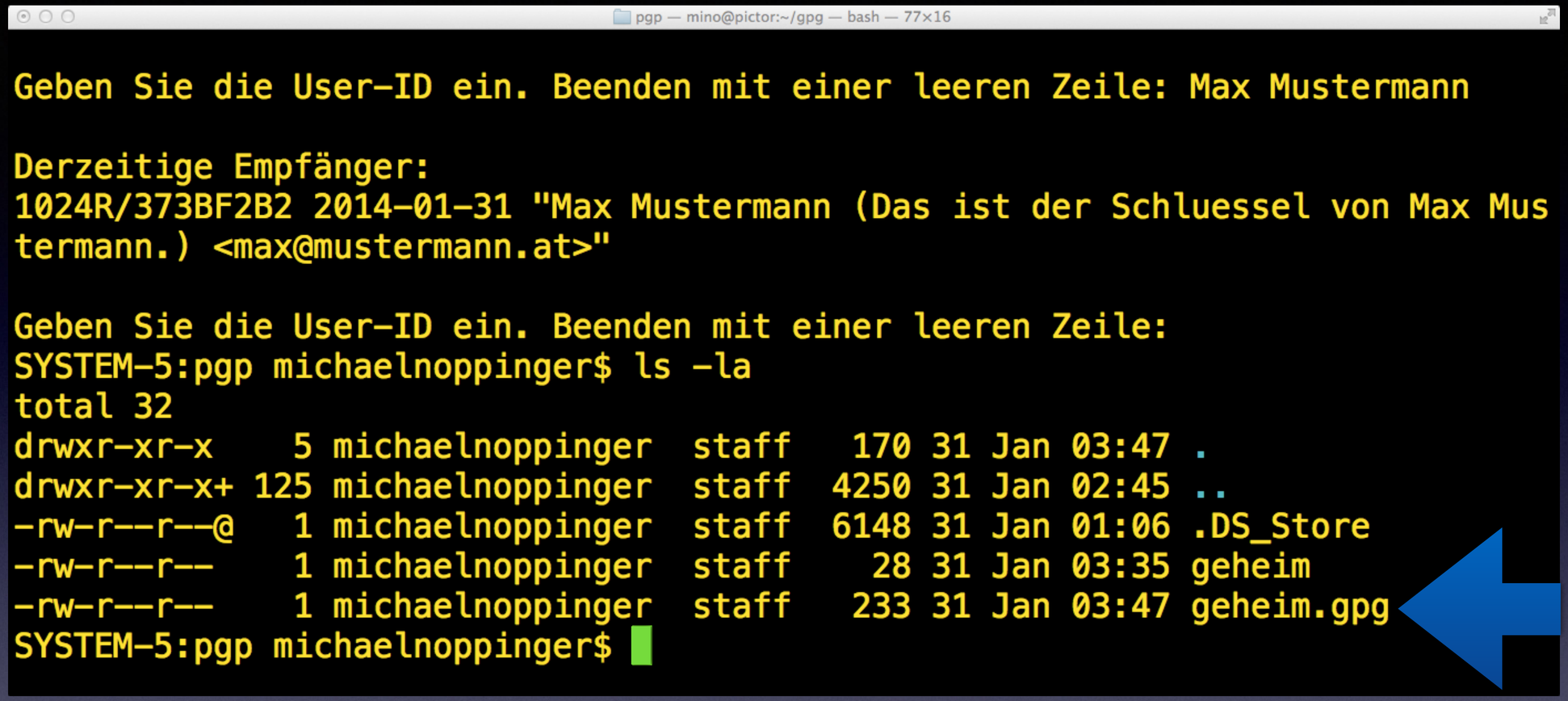
gpg -e[Datei] Empfänger

Verschlüsseln



gpg -e[Datei] Empfänger

Verschlüsseln

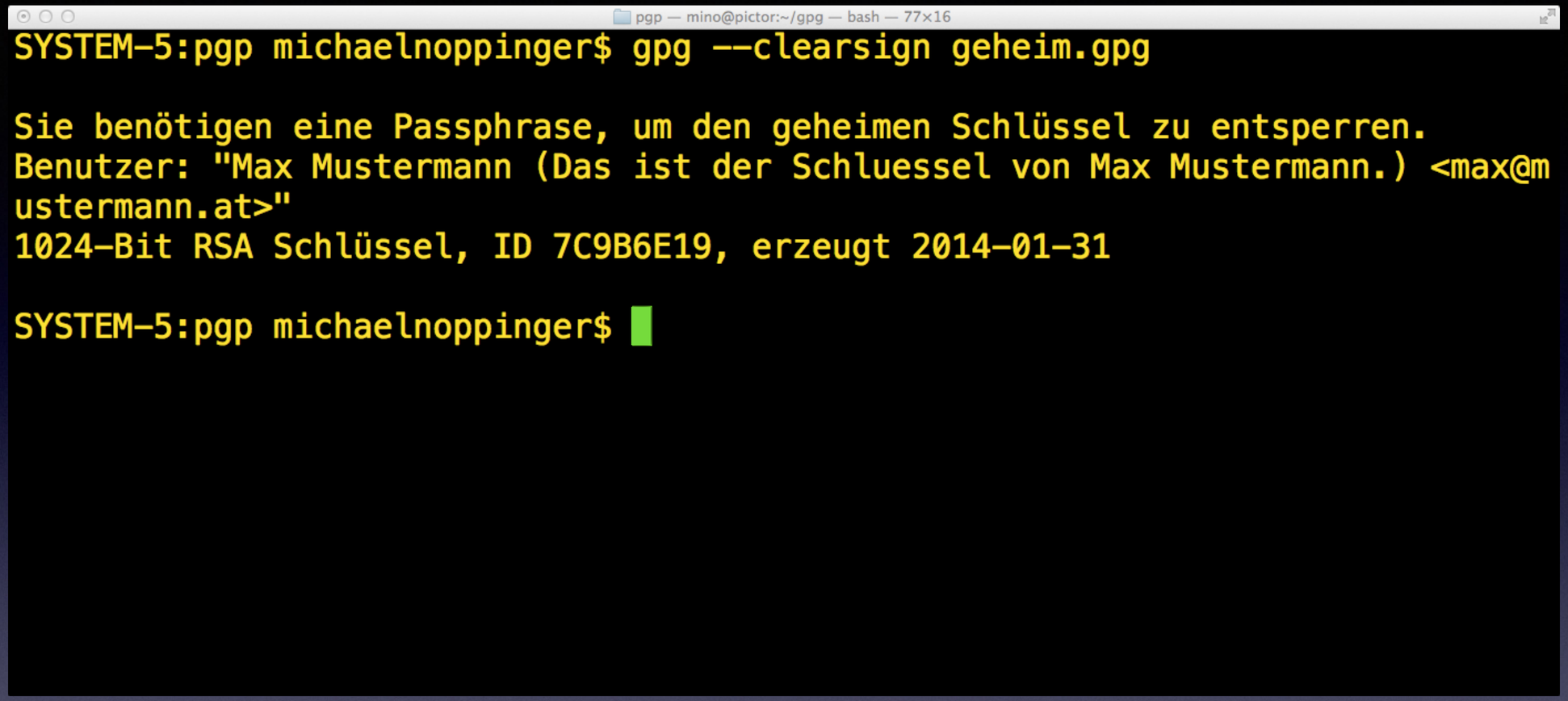


gpg -e Empfänger [Datei]

Verschlüsseln

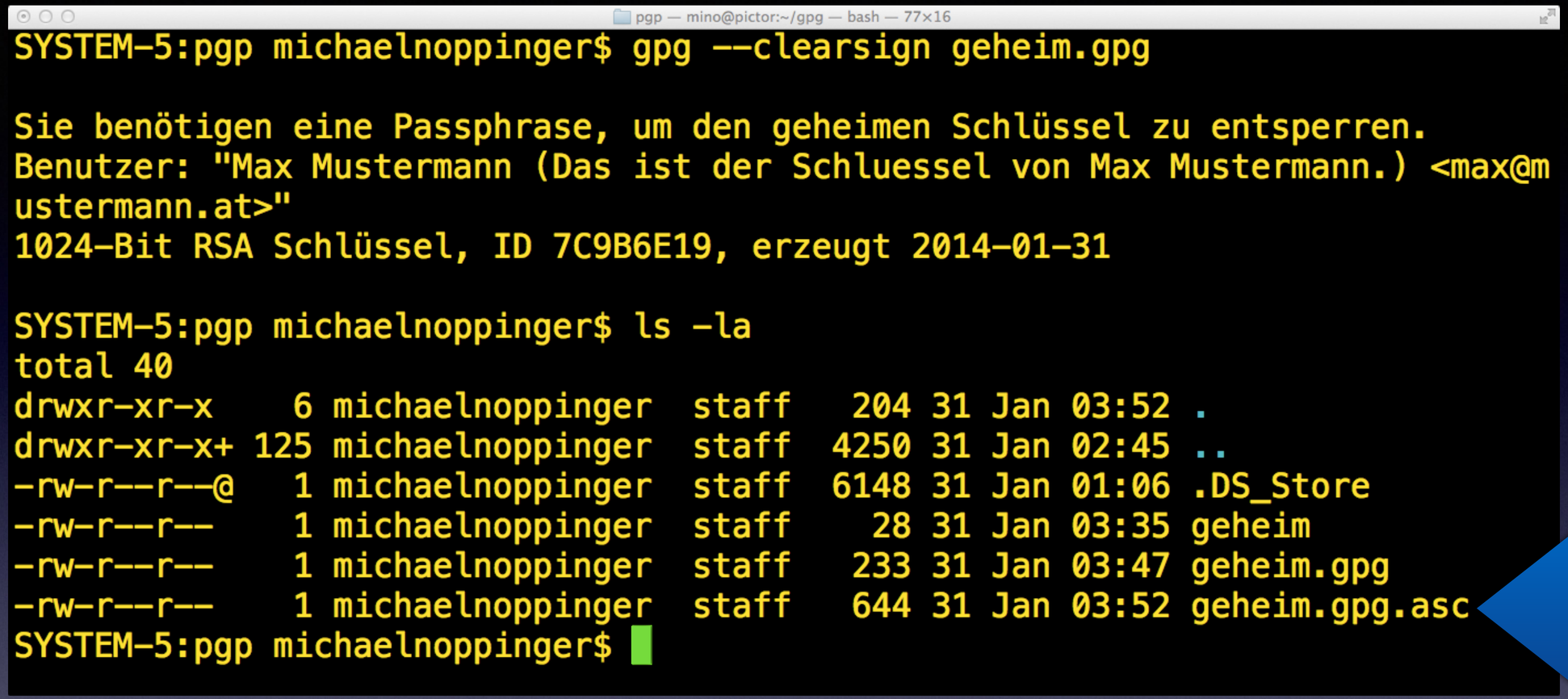
gpg --clearsign [Datei]

Dateien unterschreiben



gpg --clearsign [Datei]

Dateien unterschreiben



gpg --clearsign [Datei]

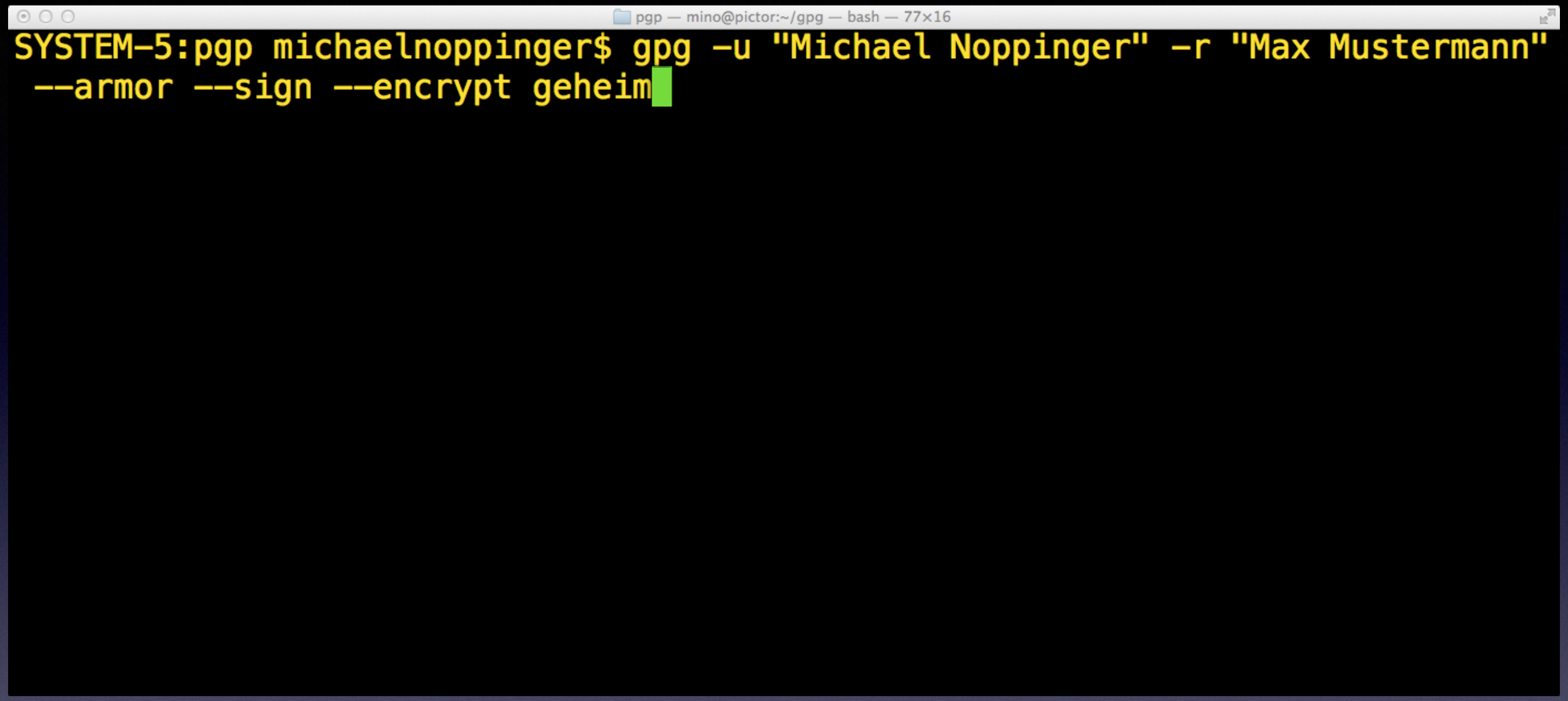
Dateien unterschreiben

gpg [--verify] [Datei]

Unterschrift verifizieren

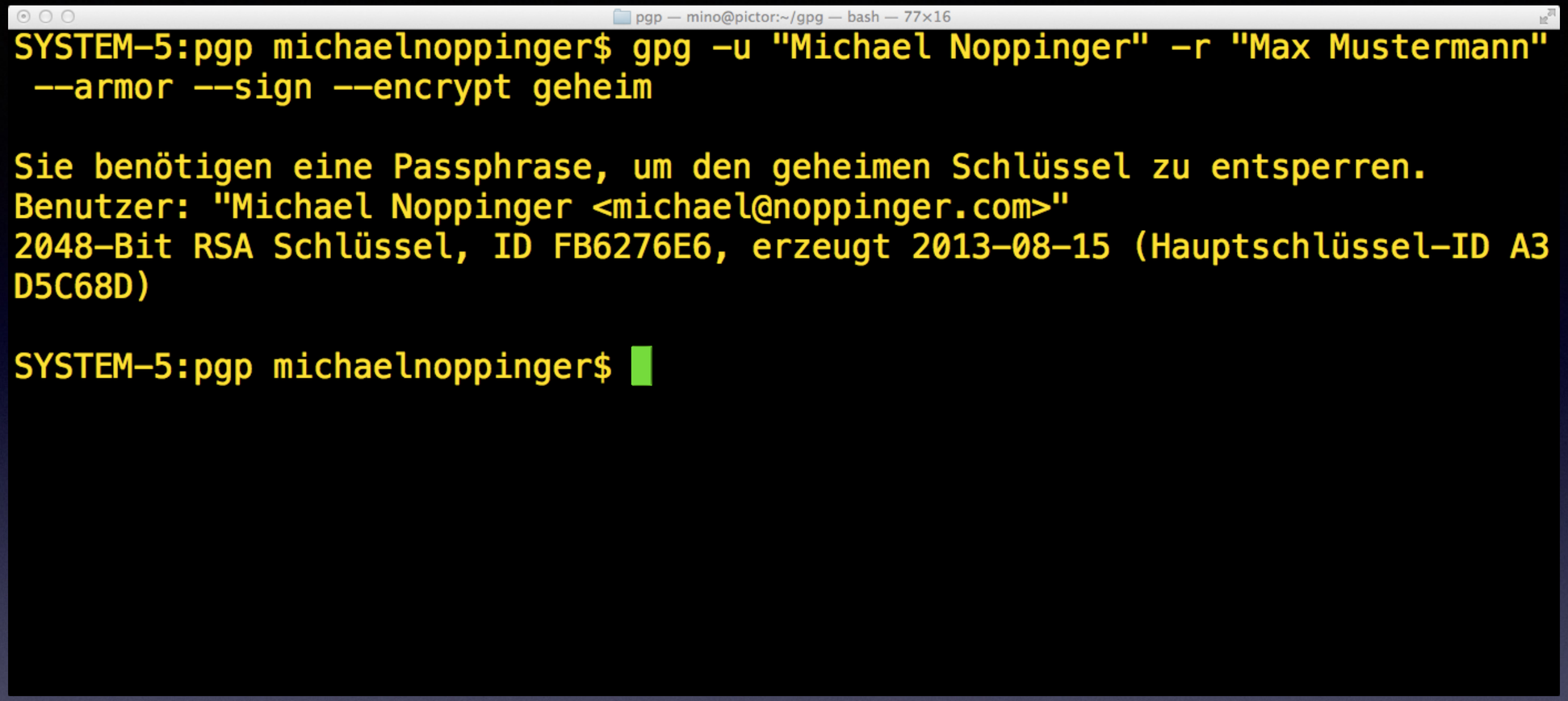
gpg [--verify] [Datei]

Unterschrift verifizieren



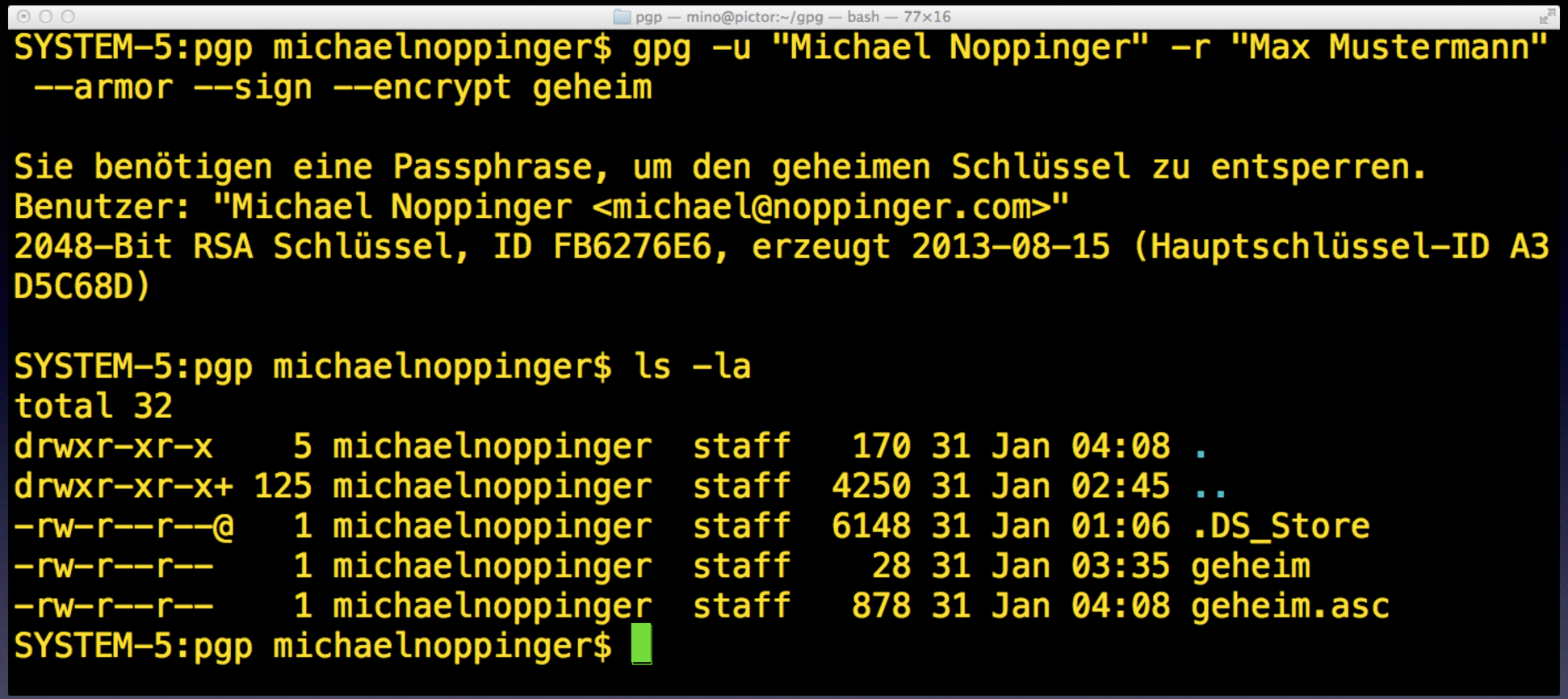
gpg [-u Sender] [-r Empfänger] [--armor] --sign --encrypt [Datei]

Signieren und Verschlüsseln



gpg [-u Sender] [-r Empfänger] [--armor] --sign --encrypt [Datei]

Signieren und Verschlüsseln



gpg [-u Sender] [-r Empfänger] [--armor] --sign --encrypt [Datei]

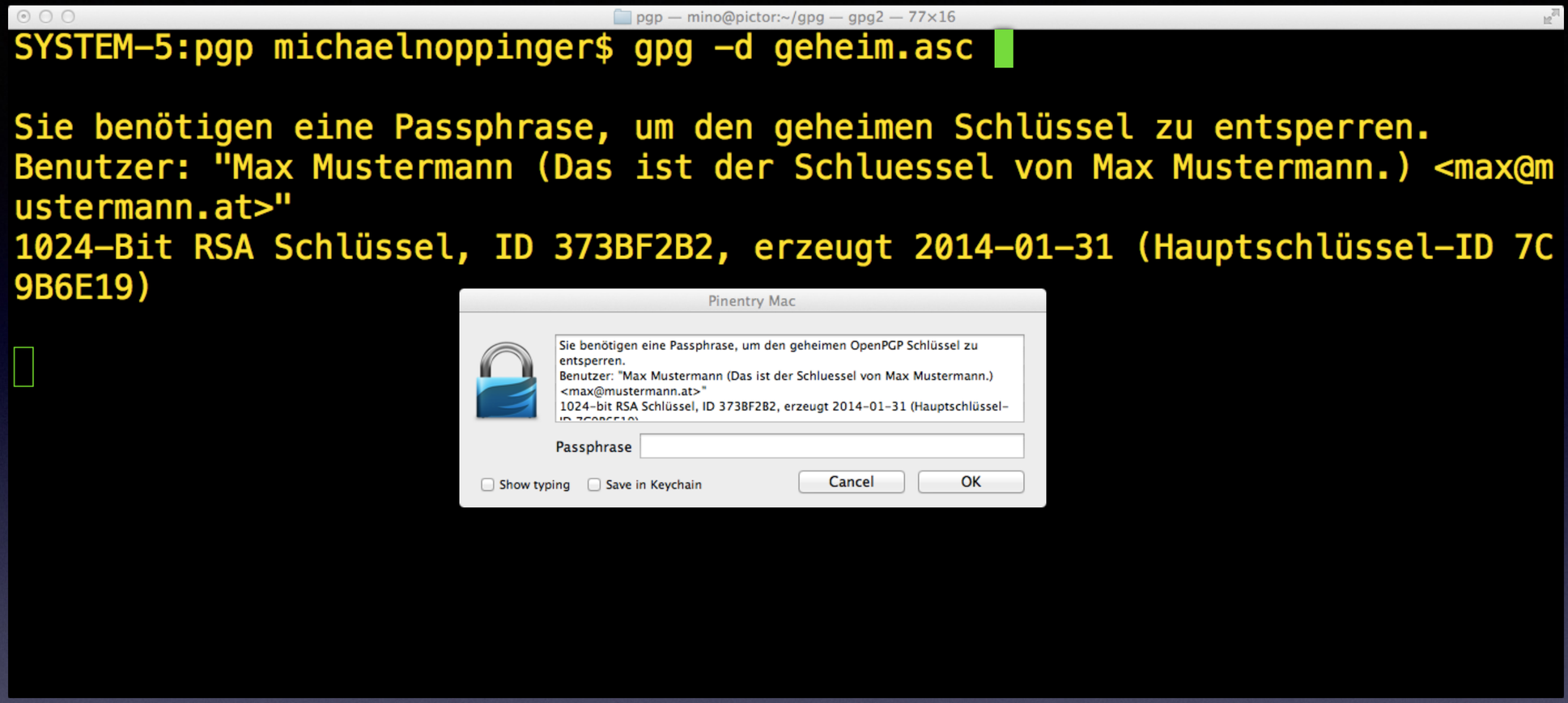
Signieren und Verschlüsseln

Inhalt von „geheim“

Inhalt von verschlüsseltem und signiertem „geheim“

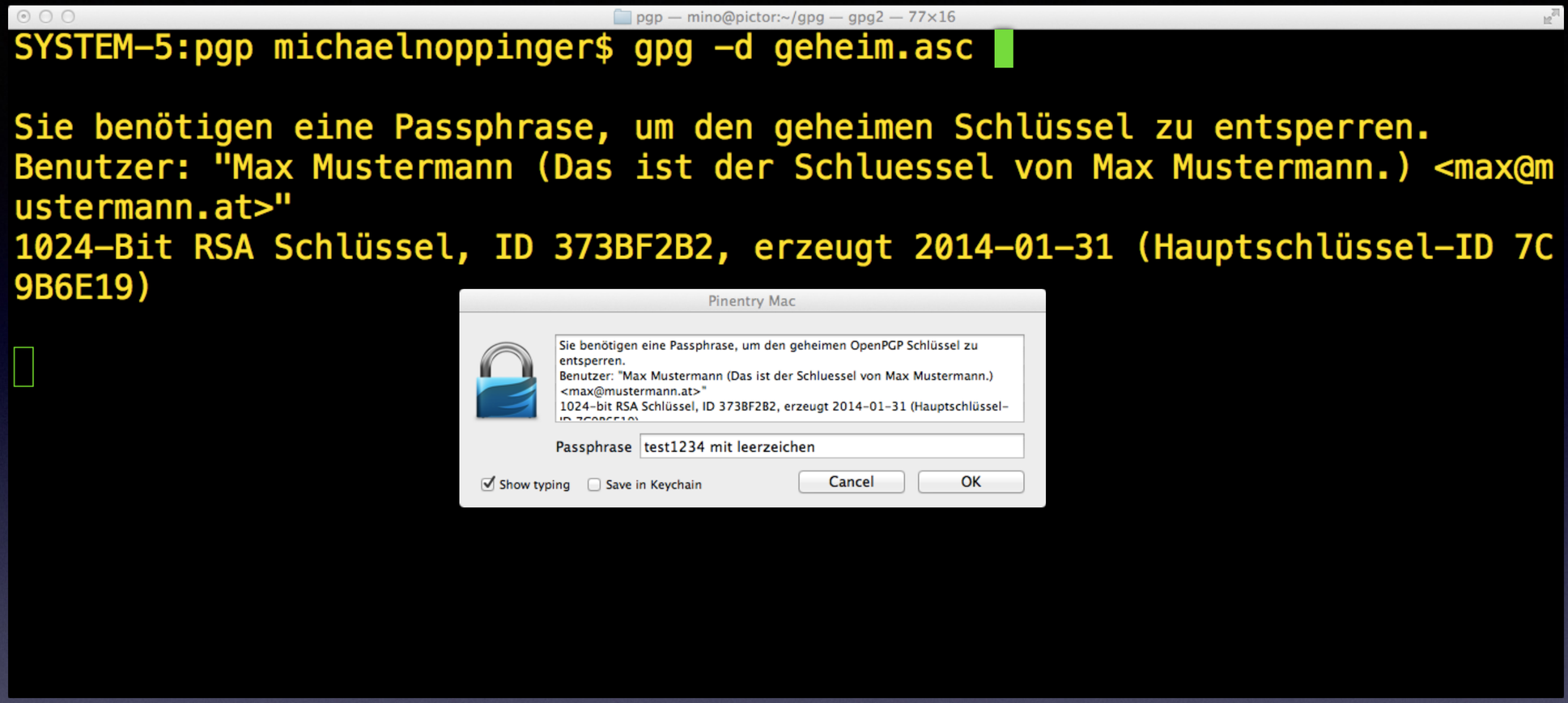
gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen



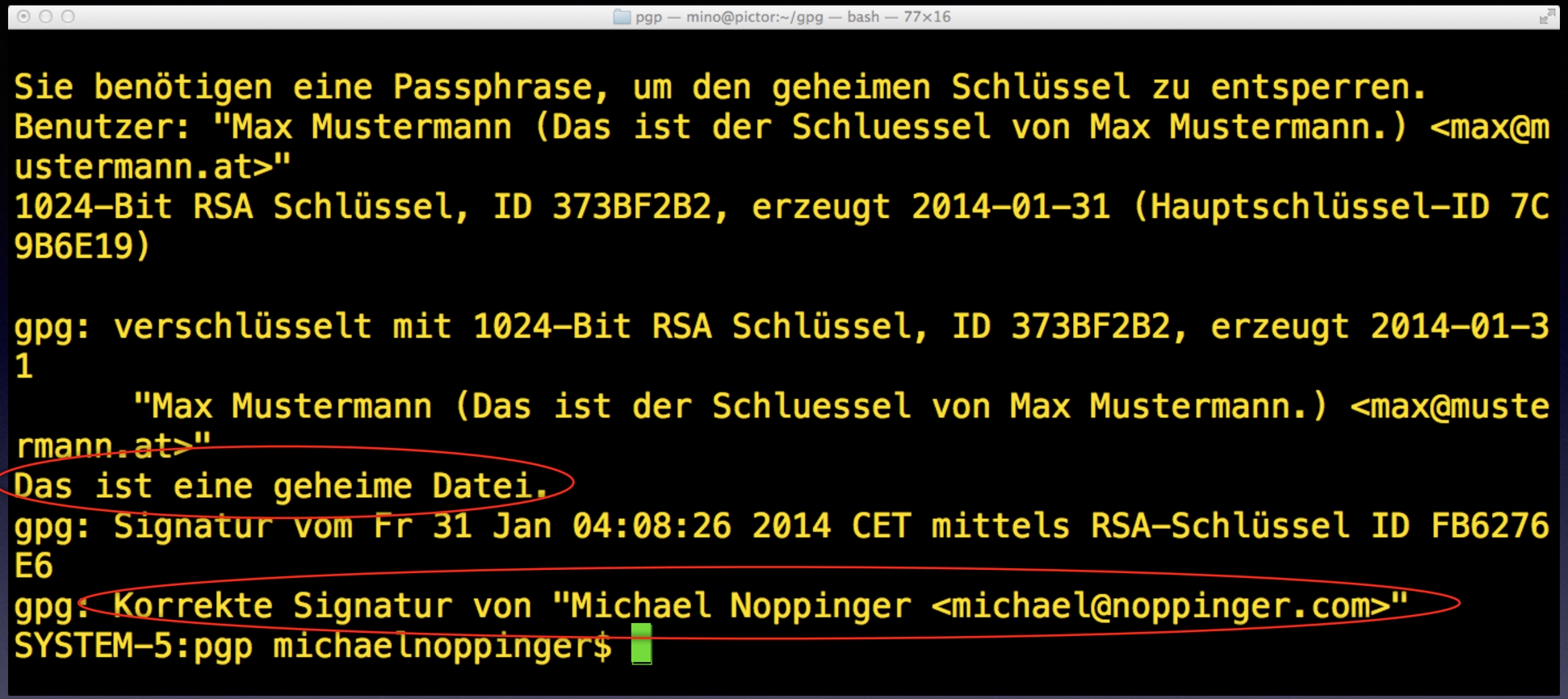
gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen



gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen



gpg [-d] [Datei]

Entschlüsseln und Signatur überprüfen

Wir wünschen viel Vergnügen
beim Ausprobieren von GnuPG!

- B. Schneier, “Applied Cryptography, Second Edition”, Wiley, 1996
  Deutsche Ausgabe unter dem Titel “Angewandte Kryptographie”, Addison-Wesley, 1996

- http://en.wikipedia.org/wiki/Gnupg