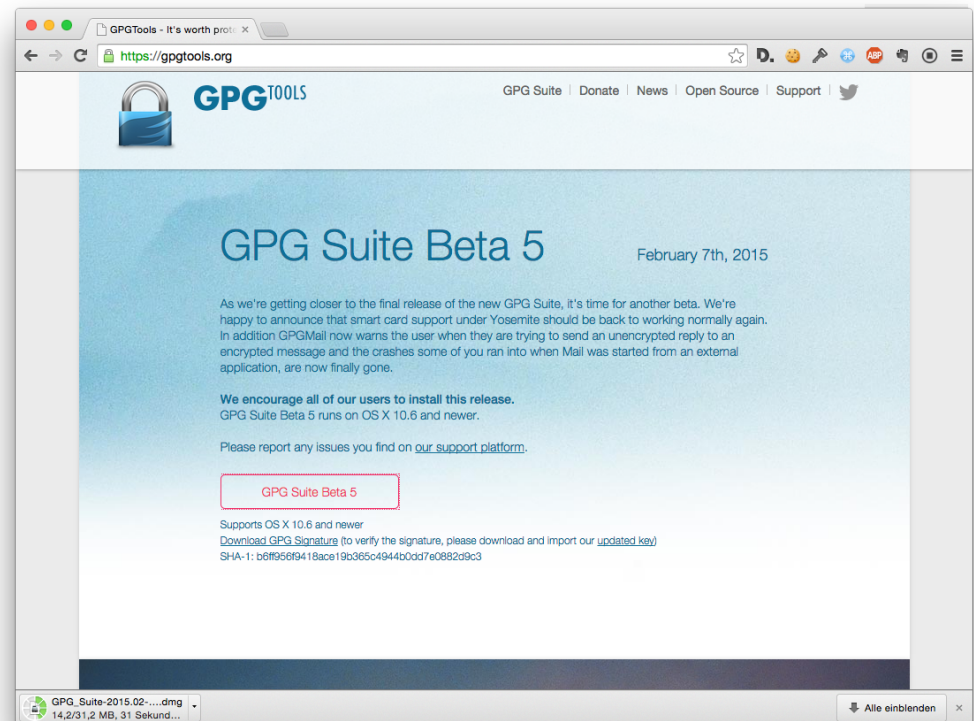


openHPI Tutorial
GPGTools für Mac OS X

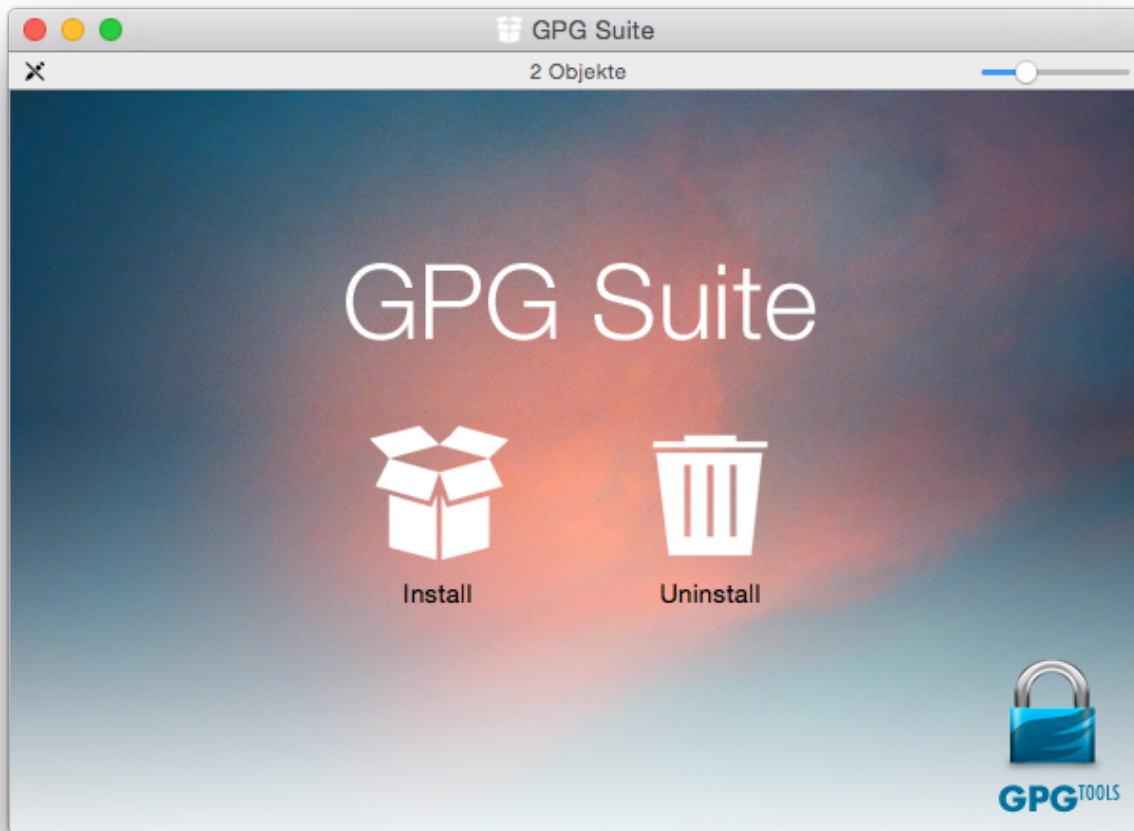
GPGTools / GPG Suite ist GPG-Komplettpaket für Mac OS X

Besteht aus:

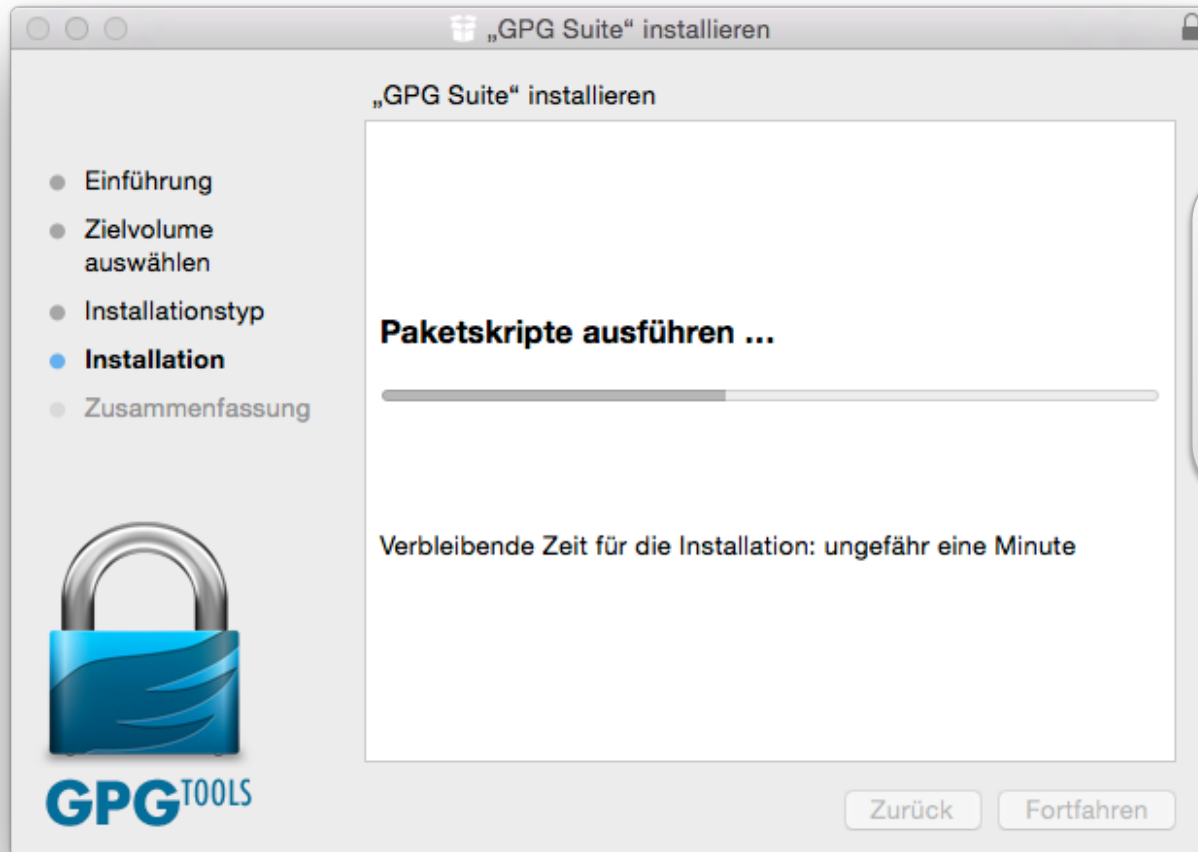
- **GPG Keychain Access:** Zertifikatsmanager
- **GPGMail:** Erweiterung für Apple Mail
- **GPGServices:** Finder-Erweiterung für Dateiverschlüsselung
- **MacGPG:** Portierung von GnuPG für OS X
- Derzeit noch kostenlos, zukünftige Versionen gegen kleine Gebühr
- Download unter <https://gpgtools.org>



- Öffnen Sie nach dem Download von <https://gpgtools.org> den Installer

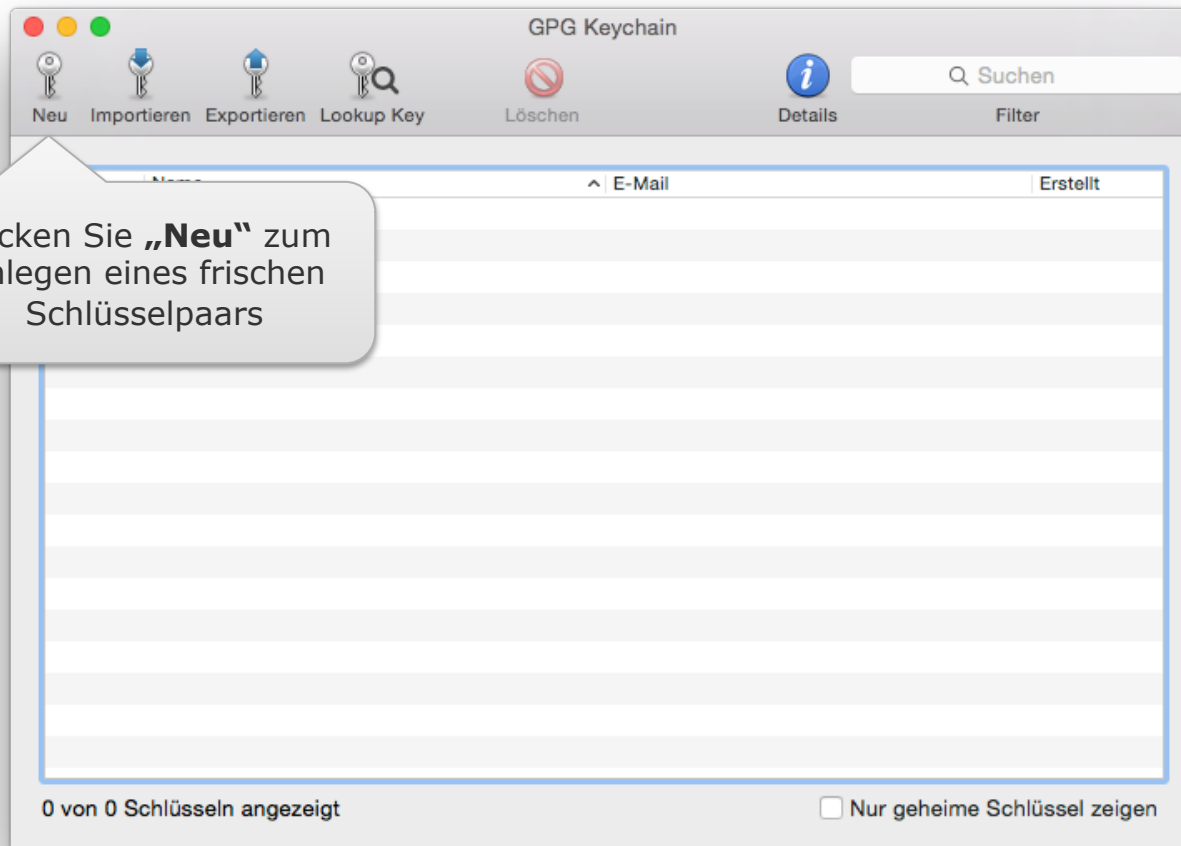


- Folgen Sie den Anweisungen im Installationsdialog



Gewöhnlich sind bei der Installation **keine Abweichungen** von den vorgegebenen Parametern notwendig.

- Öffnen Sie die Schlüsselbundverwaltung **GPG Keychain** (via Spotlight oder im Finder im Ordner „Programme“)



- Geben Sie Ihren Namen und die Email-Adresse an, mit der Sie verschlüsselt kommunizieren wollen

Ein neues Schlüsselpaar erstellen, das zum Verschlüsseln, Signieren und Beglaubigen verwendet werden kann.

Voller Name:

E-mail-Adresse:

☐ Upload public key

► Erweiterte Optionen

Passphrase:

Confirm:

0 von 0 Schlüsseln angezeigt ☐ Nur geheime Schlüssel zeigen

Die Passphrase müssen Sie jedes mal eingeben, wenn Sie Entschlüsseln oder Signieren wollen

- Geben Sie Ihren Namen und die Email-Adresse an, mit der Sie verschlüsselt kommunizieren wollen

Ein neues Schlüsselpaar erstellen, das zum Verschlüsseln, Signieren und Beglaubigen verwendet werden kann.

Voller Name:

E-mail-Adresse:

☐ Upload public key

► Erweiterte Optionen

Passphrase:

Confirm:

0 von 0 Schlüsseln angezeigt ☐ Nur geheime Schlüssel zeigen

Die Passphrase müssen Sie jedes mal eingeben, wenn Sie Entschlüsseln oder Signieren wollen

Generierung eines Schlüsselpaars (2/4)

Ein neues Schlüsselpaar erstellen, das zum Verschlüsseln, Signieren und Beglaubigen verwendet werden kann.

Voller Name: Christian Willems

E-mail-Adresse: christian.willems@hpi.de

☒ Upload public key

Erweiterte Optionen

Kommentar:

Schlüsselart: RSA und RSA (voreingestellt)

Länge: 4096

☒ Schlüssel läuft ab

Gültig bis: 16. 2.2019

Passphrase:

Confirm:

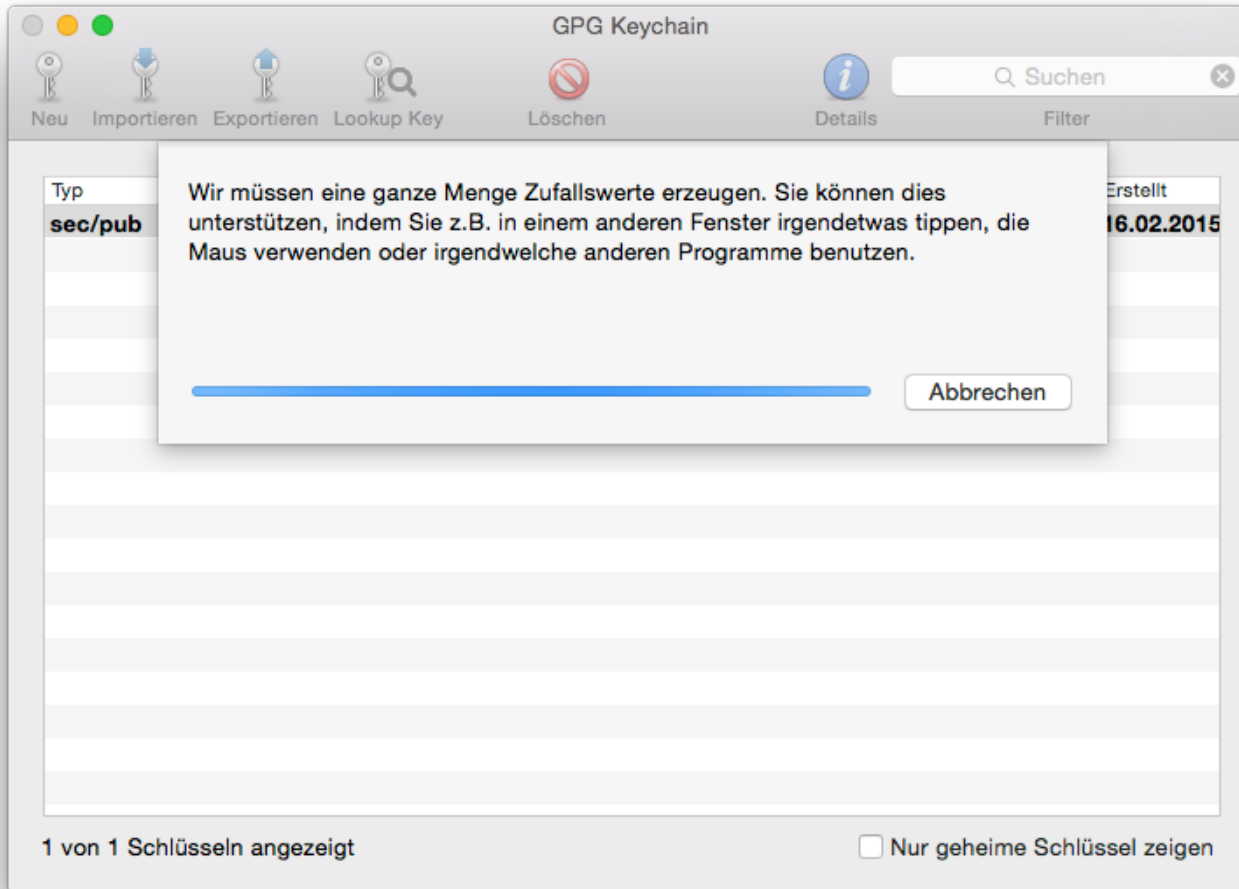
Abbrechen Schlüssel erstellen

0 von 0 Schlüsseln Schlüssel zeigen

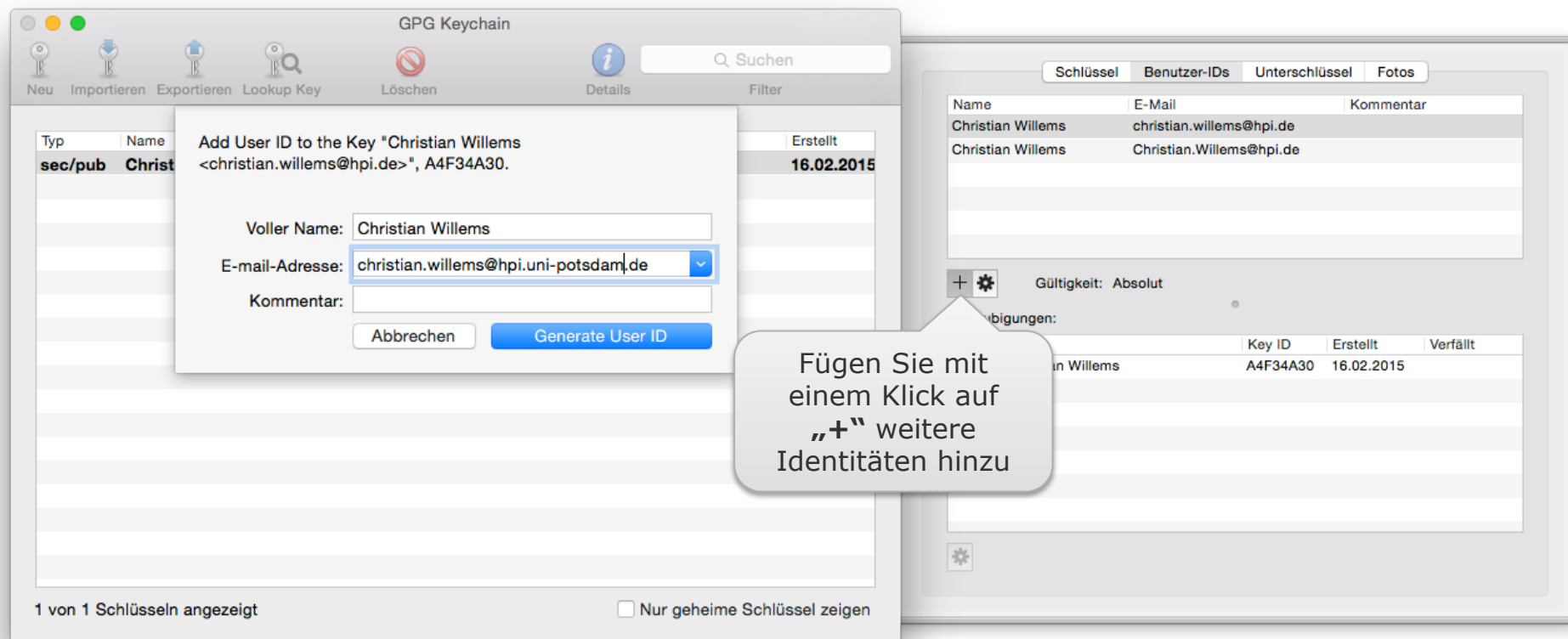
Hier können Sie die vorgegebenen Werte verwenden

Setzen Sie diesen Haken, wenn Sie Ihren Schlüssel auf einen Schlüsselservers veröffentlichen möchten

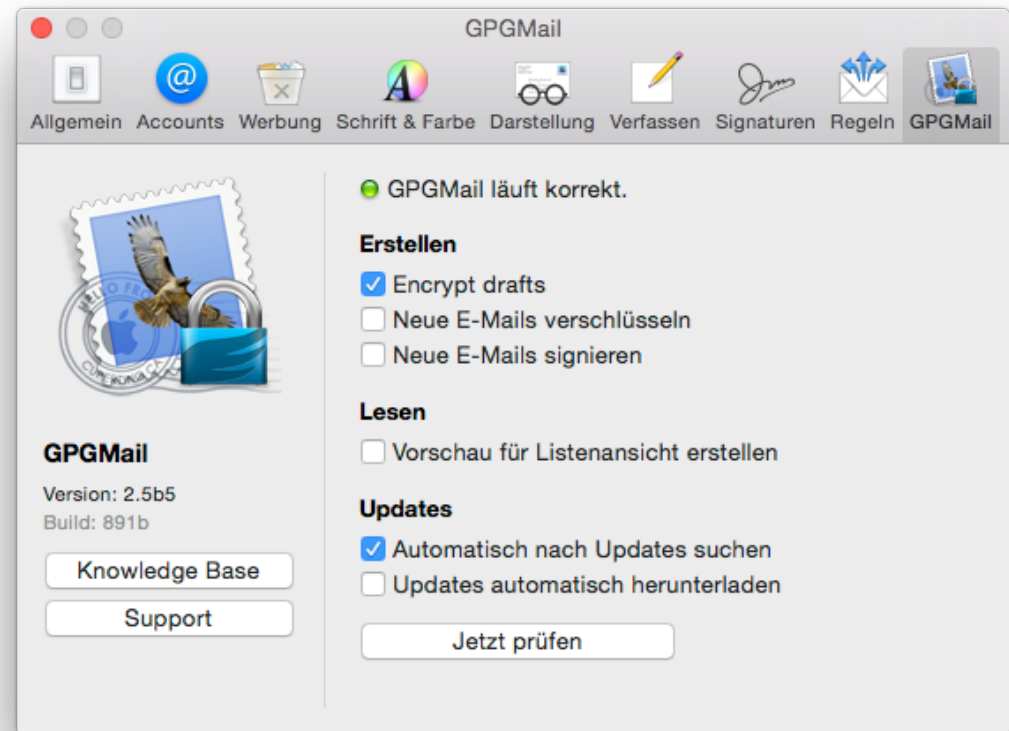
- GPG Keychain generiert jetzt die Zufallszahlen für Ihr Schlüsselpaar



- Sie können auch weitere Identitäten (Name + Email-Adresse) zu Ihrem Schlüsselpaar hinzufügen (hier: alternative Email-Adresse)
 - Öffnen Sie das „Details“-Menü
 - Wählen Sie den Reiter „Benutzer-IDs“

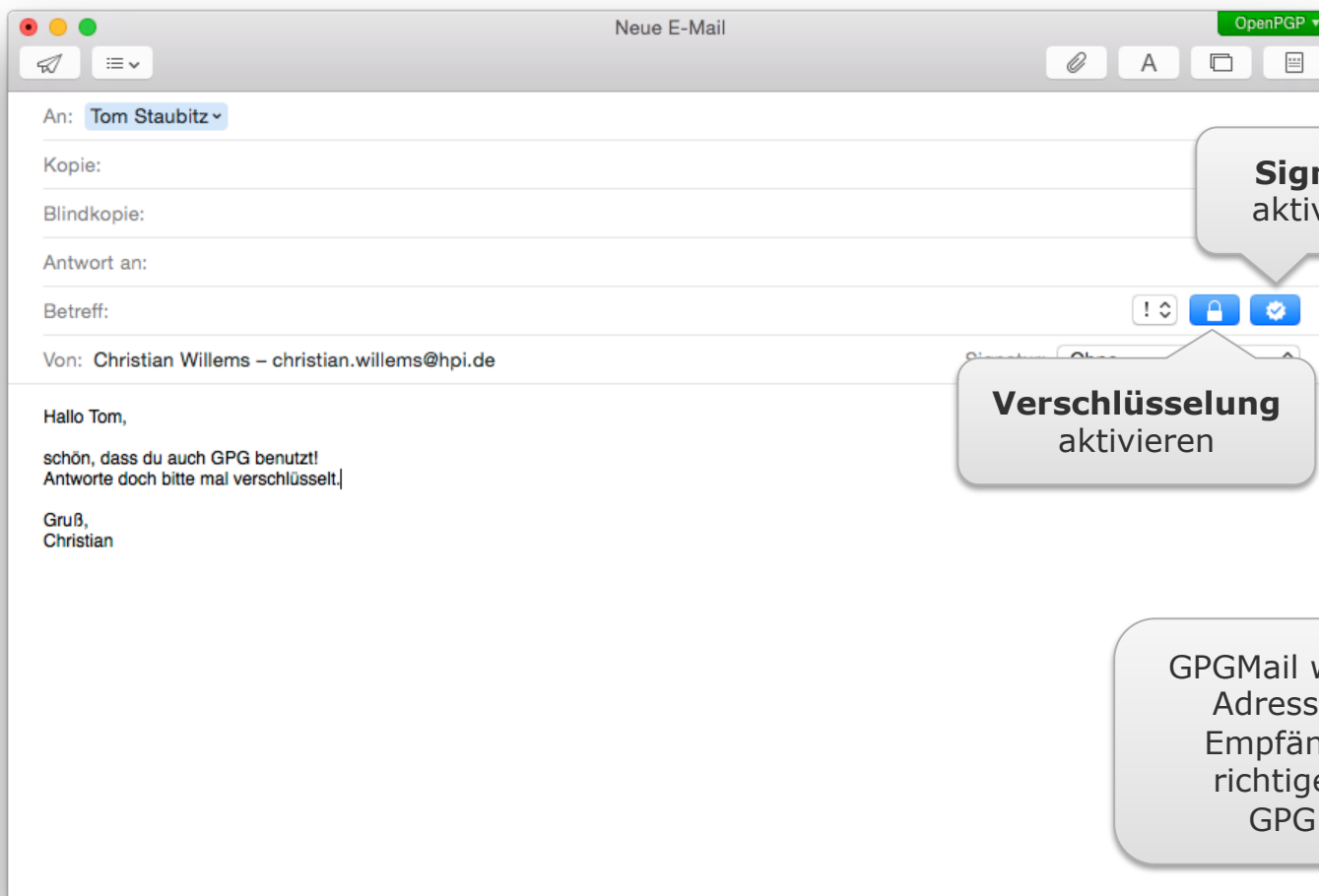


- GPG ist nach der Installation automatisch in Apples Mail-Programm integriert und hat dort eigene Einstellungen
 - Apple Mail öffnen
 - Einstellungen öffnen: ⌘+,
 - Reiter „GPGMail“ auswählen
- Hier können Sie bspw. festlegen,
 - dass neue Mails *automatisch* verschlüsselt bzw. signiert werden
 - dass schon *Entwürfe* verschlüsselt werden sollen
 - dass eine *unverschlüsselte* Vorschau für die Listenansicht erstellt wird



Versenden einer verschlüsselten und signierten Mail

- Zum Verschlüsseln benötigt man natürlich den öffentlichen Schlüssel des Empfängers



Signatur
aktivieren

Verschlüsselung
aktivieren

GPGMail wählt anhand der Email-Adressen von Absender und Empfänger **automatisch** die richtigen Schlüssel aus dem GPG Schlüsselbund aus

Empfang einer verschlüsselten und signierten Mail

- Auch hier: zum Prüfen der Signatur benötigt man den öffentlichen Schlüssel des Absenders

