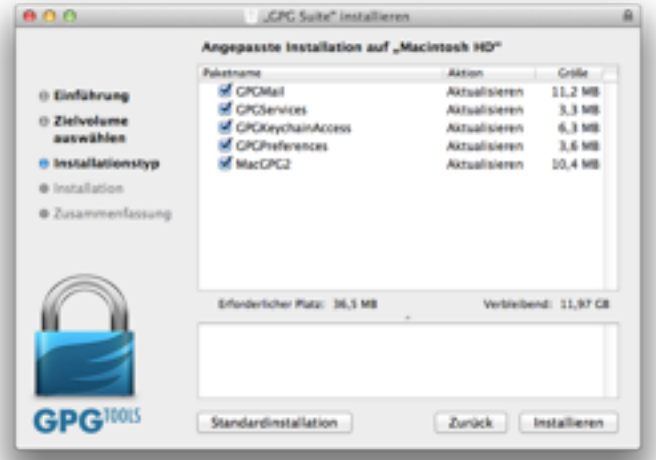
GPGTools und Apple Mail auf Mac OS 10.9

Eine ältere deutschsprachige Beschreibung mit weiterführenden Links und Informationen zum Thema E-Mailverschlüsselung findet sich unter <http://www.macon.cc/blog/2011/12/e-mail-verschlusselung-unter-mac-os-x/>.

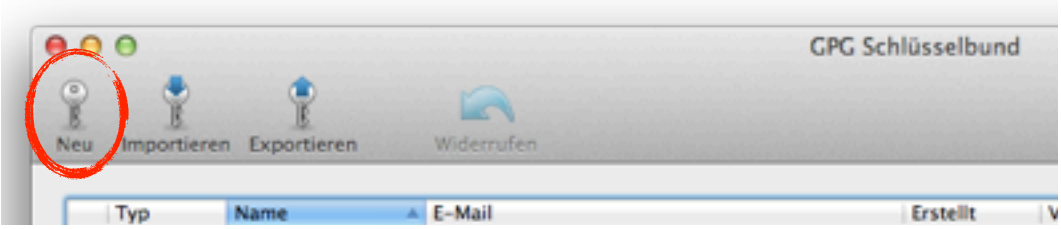
Mit GPGTools E-Mail signieren und verschlüsseln

Sie können die neueste Version der GPG Suite von der Seite <https://gpgtools.org/#gpgsuite> herunterladen. Installieren Sie die GPG Suite.

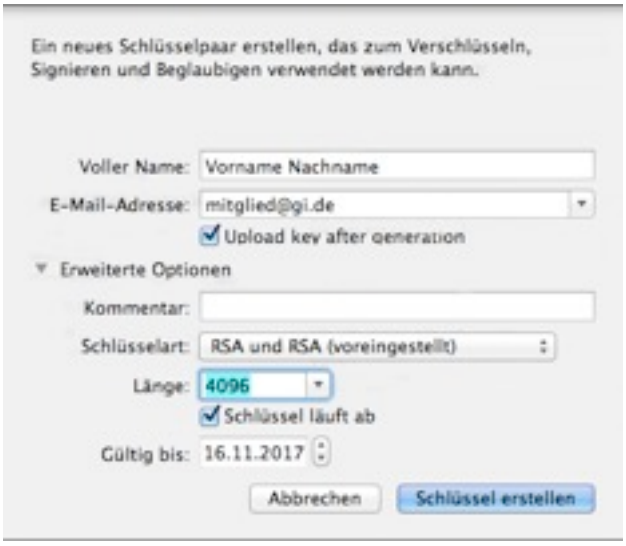


Schlüsselpaar erzeugen

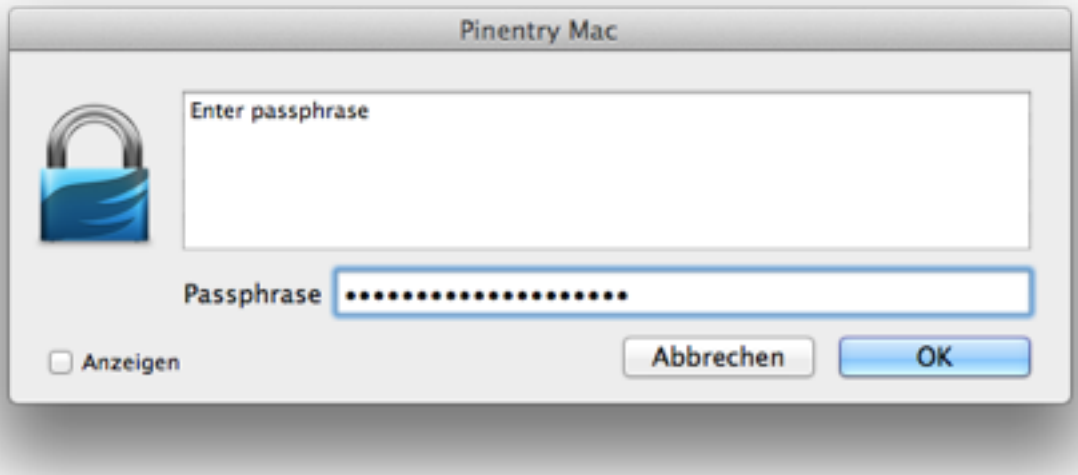
Öffnen Sie nach erfolgreicher Installation den GPG-Schlüsselbund. Dort können Sie ein neues Schlüsselpaar erstellen, indem Sie auf »Neu« klicken.



Es öffnet sich ein Dialog, in dem Sie Ihren Namen und E-Mailadresse eintragen können, für welche das Schlüsselpaar verwendet werden soll. Sie können zwischen RSA und DSA als Schlüsselart wählen, wobei sich RSA mit einer Schlüssellänge von 4096 Bit empfiehlt. Auch können Sie ein Verfallsdatum wählen, um die Sicherheit zu erhöhen.

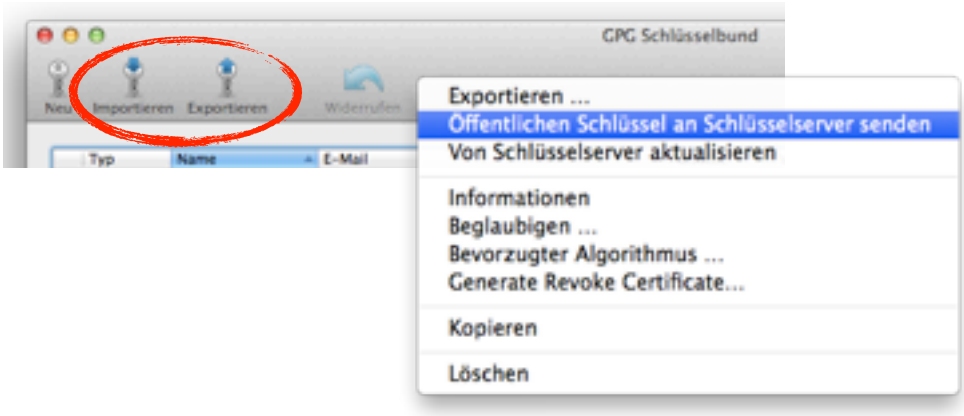


Wenn Sie »Schlüssel erstellen« auswählen, werden Sie 2x nach einer Passphrase gefragt. Bitte wählen Sie Ihre Passphrase sorgfältig [vgl. dazu Schneier[1] : »*Finally, there are two basic schemes for choosing secure passwords: the Schneier scheme and the XKCD scheme.*«].



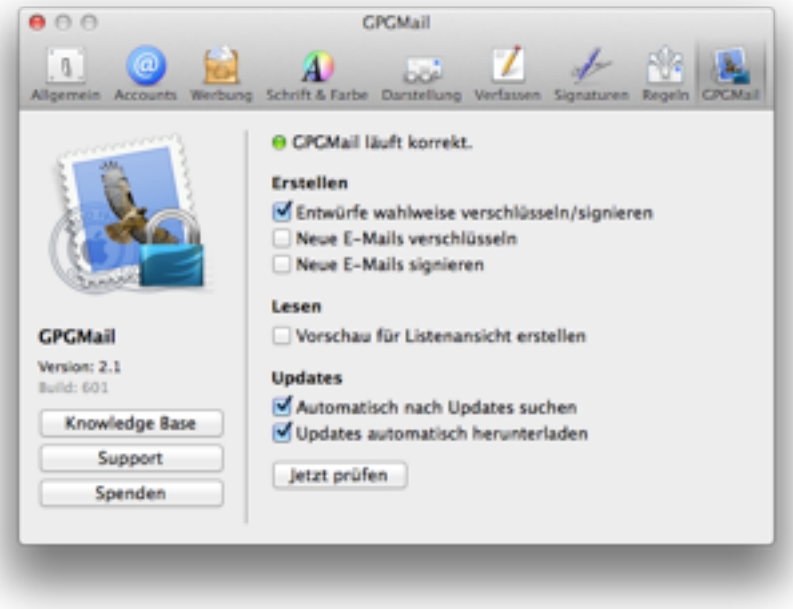
Nun wird das Schlüsselpaar erzeugt, was eine gewisse Zeit in Anspruch nimmt. Während dieser Zeit empfiehlt es sich, den Rechner normal zu benutzen, um bessere Werte für den Zufallsgenerator zu erzeugen, der an der Erstellung des Schlüsselpaares beteiligt ist.

[1] siehe https://www.schneier.com/blog/archives/2012/09/recent_developm_1.html.



Ihren öffentlichen Schlüssel können Sie dadurch in Umlauf bringen, dass Sie ihn entweder auf einen der eingetragenen Schlüsselserver hochladen (Rechtsklick zum Kontextmenü oder über das Hauptmenü »Schlüssel > An Schlüsselserver senden«) oder exportieren und als Textdatei zur Verfügung stellen. Bitte exportieren und stellen Sie ausschließlich ihren öffentlichen Schlüssel zur Verfügung.

Um den öffentlichen Schlüssel eines Kommunikationspartners im Schlüsselbund zu sichern, können Sie entweder einen der Schlüsselserver abfragen (Hauptmenü »Schlüssel > Von Schlüsselserver abfragen«) oder den öffentlichen Schlüssel direkt importieren. Die Schlüsselserver können Sie im Hauptmenü unter »GPG Schlüsselbund > Einstellungen… > Schlüsselserver« auswählen oder ändern.



Apple Mail-Einstellungen

In den Apple Mail-Einstellungen ist durch die Installation der GPG Suite der Menüpunkt »GPGMail« hinzugekommen. Dort können Sie u. a. einstellen, ob Mails automatisch signiert oder verschlüsselt werden.

E-Mail signieren/verschlüsseln

Sofern Mail Ihre Mails nicht automatisch signieren oder verschlüsseln soll, erfordert das Signieren und Verschlüsseln der Mail jeweils einen Klick. Klicken Sie auf das Schloss, wenn Sie verschlüsseln und/oder auf das Signatursymbol, wenn Sie signieren möchten. Zum Verschlüsseln benötigen Sie den öffentlichen Schlüssel Ihres Kommunikationspartners. Sie sehen anhand des Symbole sofort, ob Sie eine der Optionen ausgewählt haben. Außerdem erscheint das OpenPGP-Symbol in dem Fall grün. Sie können nun Ihre Mail signiert und/oder verschlüsselt wie gewohnt versenden.