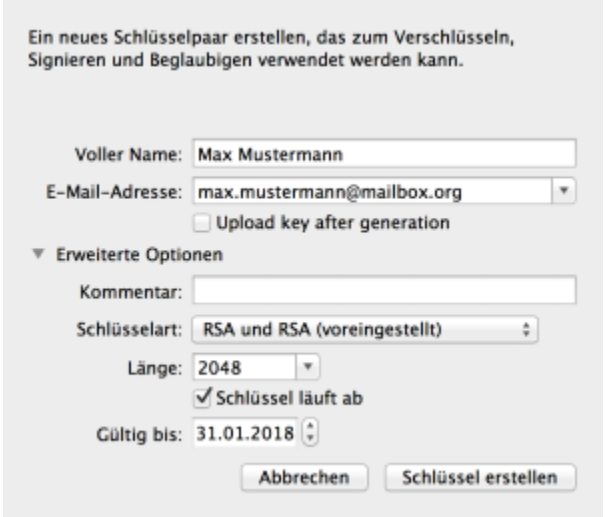
PGP-Einrichtung unter Mac OS X

Zur Verschlüsselung von E-Mails mit „**Apple Mail**“ unter OS X verwenden Sie am besten die kostenpflichtige Programmsammlung „**GPG Suite**“ von der Webseite www.gpgtools.org. Laden Sie dort die aktuelle Version der „**GPG Suite**“ herunter und installieren es auf Ihrem Mac. Alle notwendigen Programme sind in diesem Paket enthalten.

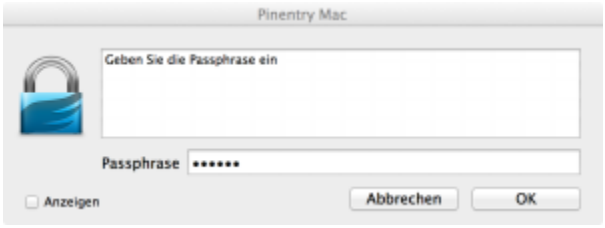
So richten Sie PGP mit der GPG Suite ein

Im ersten Dialogfeld erzeugen Sie für Ihre E-Mail-Adresse ein neues Schlüsselpaar.
Achtung: Laden Sie den neuen Schlüssel **nicht** sofort auf einen Schlüsselserver hoch! Stellen Sie sicher, dass die Option „Upload key after generation“ nicht ausgewählt ist.
Der Hintergrund ist, dass ein veröffentlichter PGP-Schlüssel nicht mehr (von den Schlüsselservern) gelöscht werden kann. Laden Sie den neuen Schlüssel nur dann auf einen Schlüsselserver, wenn Sie sich sicher sind, dass Sie diesen Schlüssel benutzen wollen.

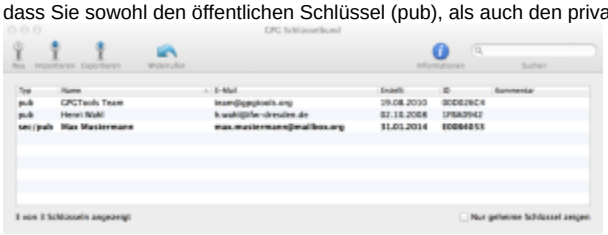


Ebenso ist es sinnvoll, den Schlüssel mit einem Ablaufdatum zu versehen. Da sich die Technik der Schlüsselerzeugung im Laufe der Zeit entwickelt (genau wie die Anforderungen an sichere Verschlüsselungsverfahren), sollte der Schlüssel nach einiger Zeit neu erzeugt werden, damit er auch zukünftig als sicher gelten kann. Zwei bis fünf Jahre sind hier ein guter Wert.

Wurde das Schlüsselpaar erstellt, dann sichern Sie Ihren privaten Schlüssel mit einem Passwort. Dieses Passwort benötigen Sie fortan, um E-Mails zu ver- oder entschlüsseln:



Wenn Sie das erledigt haben, wird Ihnen im Programm „**GPG Schlüsselbund**“ das neue Schlüsselpaar angezeigt. „**sec / pub**“ ist der Hinweis darauf, dass Sie sowohl den öffentlichen Schlüssel (pub), als auch den privaten Schlüssel (sec) besitzen.



Achten Sie darauf, dass Ihnen dieses Schlüsselpaar nicht abhanden kommt! Wenn Sie es verlieren, können Sie die damit verschlüsselten E-Mails und Daten nicht mehr entschlüsseln! Wir empfehlen Ihnen, Ihr PGP-Schlüsselpaar zu „**Exportieren**“ und z.B. auf einem externen Datenträger oder in einer verschlüsselten Container-Datei als Kopie zu sichern.

Wenn Sie das alles erledigt haben, können Sie die „**GPG Schlüsselverwaltung**“ schließen.

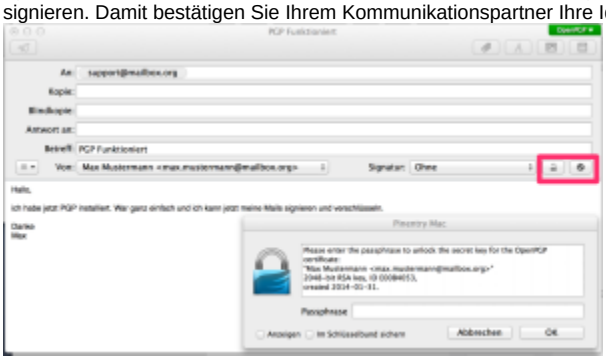
Der Schlüsselaustausch

Wenn Ihnen nun jemand eine verschlüsselte E-Mail schicken möchte, benötigt er dafür Ihren öffentlichen PGP-Schlüssel. Für die Übermittlung des Schlüssels gibt es mehrere Möglichkeiten.

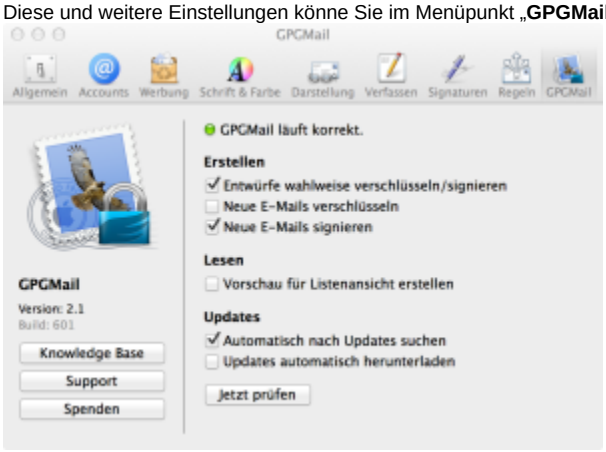
- Am einfachsten ist es, wenn Sie Ihren öffentlichen Schlüssel auf einen sogenannten Schlüsselserver hochladen. Von dort können Ihn andere E-Mail-Nutzer herunterladen und Ihnen so leicht eine verschlüsselte E-Mail schicken. Zum Hochladen klicken Sie in der Menüleiste der „**GPG Schlüsselverwaltung**“ auf „**Schlüssel**“ und dann auf „**An Schlüsselserver senden**“. Über das selbe Menü können Sie auch die öffentlichen Schlüssel anderer Nutzer auf dem Schlüsselserver suchen, z.B. wenn Sie jemandem eine verschlüsselte E-Mail schicken möchten. Klicken Sie in diesem Fall einfach auf „**Nach Schlüssel suchen**“.
- Sie können Ihren öffentlichen Schlüssel auch mit einer signierten E-Mail an Ihr Gegenüber schicken.
- Alternativ können Sie Ihren Schlüssel auch auf Ihrer Webseite zum Download anbieten.

Verschlüsselte / signierte E-Mails verschicken

Wenn Sie nun mit „**Apple Mail**“ eine neue E-Mail schreiben, werden Ihnen die neuen PGP-Funktionen angezeigt (siehe Screenshot). Mit dem Schloss-Symbol können Sie Ihre E-Mail verschlüsseln. Mit dem Zahnrad-Symbol signieren (unterschreiben) Sie Ihre E-Mail. Wir empfehlen, E-Mails immer zu signieren. Damit bestätigen Sie Ihrem Kommunikationspartner Ihre Identität und tragen bei zur Verbreitung sicherer Kommunikation.



Diese und weitere Einstellungen könne Sie im Menüpunkt „**GPGMail**“ vornehmen.



Übrigens: Eine gute Alternative zu „**Apple Mail**“ ist der E-Mail-Client Mozilla Thunderbird. Für Thunderbird gibt es das Plug-in Enigmail, durch das die PGP-Unterstützung einfach ermöglicht werden kann. HINWEIS: **Enigmail wird im neusten Thunderbird nicht mehr unterstützt. Thunderbird bringt mit OpenPGP eine eigene Verschlüsselung raus. Ab Thunderbird 78 wirksam.**

Verwandte Artikel

- Den Tor-Exit-Node von mailbox.org verwenden
- Die Zwei-Faktor-Authentifizierung einrichten
- Wie E-Mails mit PGP verschlüsselt versendet werden
- SMIME beim verschluesselten Postfach
- WebDav unter Windows