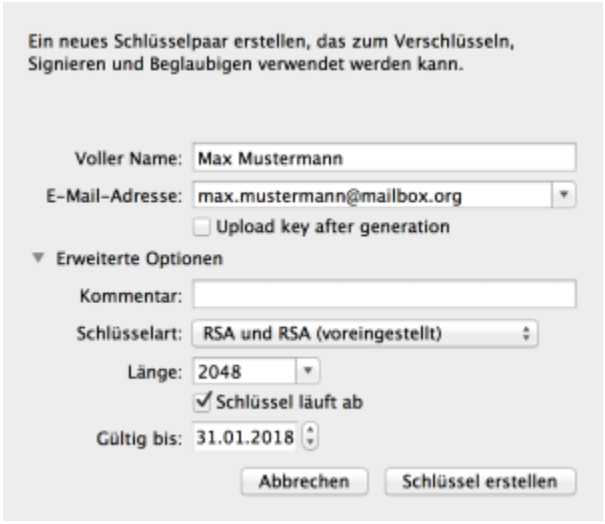
Setup GPGTools for Mac OS X

Use the GPGTools program collection available at www.gpgtools.org to encrypt e-mails using the Apple e-mail client in OS X. Download **GPG Suite** and install it on your Mac. This software contains all of the necessary tools.

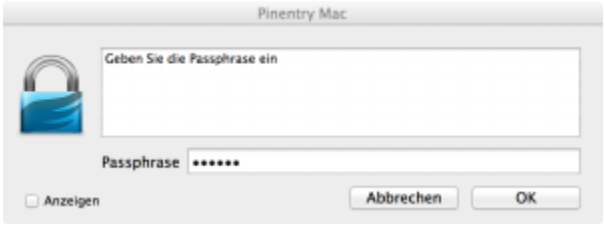
Setting up GPG with GPGTools

Create a new key pair for your e-mail address in the first dialog field. Make sure that you do not upload the new key to the key server right away. Ensure that the 'Upload key after generation' box is NOT enabled. Background information: A GPG key can no longer be deleted once it has been published. Only upload the new key to the key server once you are sure that you wish to use this key.

We also recommend giving your key an expiration date. Because key generation technology changes with time, you should generate a new key every so often so that it remains secure in the future. Your key should generally be changed every three to five years.

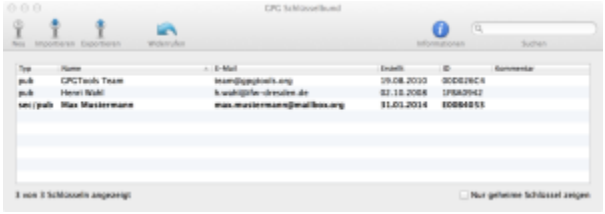


Secure your private key with a passphrase once you have created the key pair. You will need this passphrase when you wish to encrypt or decrypt e-mails.



Once you have completed this step, you will be able to see the new key pair in the program 'GPG Keychain Access'. sec/pub indicates that you have both the public (pub) key and the private (sec) key.

Make sure that you do not lose this key pair. If you lose it, you will no longer be able to read the e-mails encrypted using this key. We recommend 'exporting' your GPG key pair and storing a copy on an external data storage device.

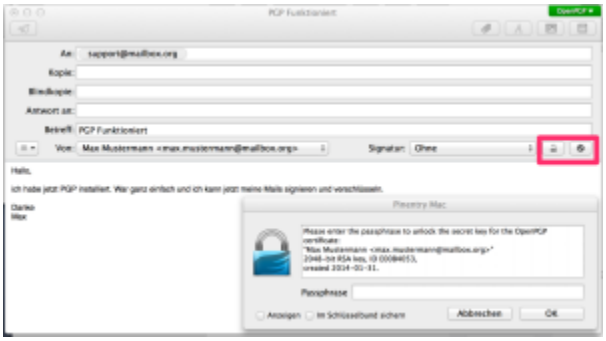


If someone would like to send you encrypted e-mails, just send them the public part of your GPG key. There are multiple ways to do this. The easiest thing to do is to upload your public key to a key server. This enables other e-mail users to find it and easily send you an encrypted e-mail. To upload your key, go to the menu bar of the GPG program and click '**Key**' and '**Send to Key Server**'. You can use the same menu to search for the public keys of other users on the key server so that you can send them encrypted e-mails as well. To do this, click '**Search for Key**'.

Alternatively, you can send your public key to the other user via a signed e-mail or allow users to download your key from your website.

Once you have completed these steps, you can close 'GPG Keychain Access'.

When you write a new e-mail in your e-mail client, you will now find the new GPG functions labeled in the program. Select the lock icon to encrypt your e-mail and select the small gear icon to sign your e-mail. We recommend always signing your e-mails. By doing this, you confirm your identity to your communication partner and help promote secure communication.



You can set up the additional functions of **GPGTools** in the settings of your e-mail client.

Tip: Mozilla Thunderbird is a good alternative to Apple Mail. The Enigmail plug-in for Thunderbird makes it easy for you to set up your e-mail client for GPG support.

Related Articles

- Drive Client on Macs, PCs, and Smartphones
- Move away from Gmail to mailbox.org - step-by-step
- How to use two-factor authentication - 2FA
- Setup with K-9 Mail for Android
- Temporary mailbox for external users