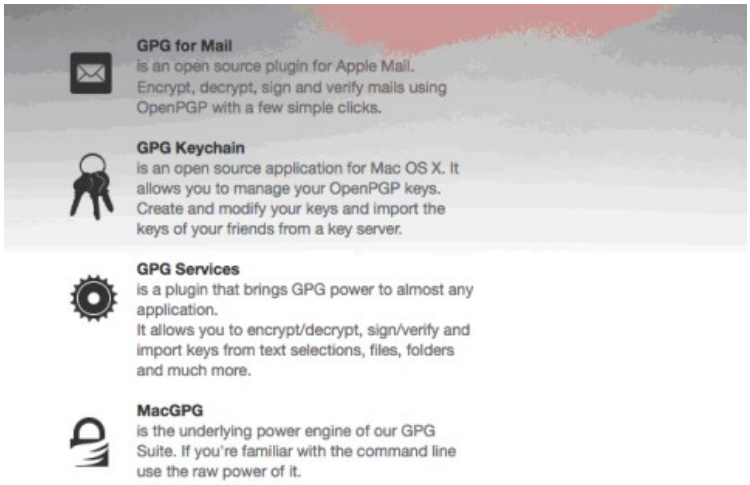
Verschlüsselung mit GPGTools for Mac

Was ist GPGTools?

GPGTools (GNU Privacy Guard) ist ein Kryptografie-Werkzeugpaket zum Verschlüsseln und Signieren unter dem Betriebssystem Apple Mac OSX. Mit GPGTools kann jeder E-Mails, Dateien und Datei-Ordner einfach und kostenlos ver- und entschlüsseln, sowie ihre Integrität (Unveränderheit) und Herkunft (Authentizität) absichern und überprüfen. GPGTools und die darin enthaltenen Komponenten sind Freie Software (OSS).

Die wesentlichen Komponenten von GPG4Win sind:



- MacGPG: Der eigentliche Kern, eine Portierung von GnuPG für OS X
- GPGMail: Ein Plugin für OS X Mail
- GPGServices: Die Komponente, um im Servicemenü von OS X Kryptofunktionen bereitzustellen (Text- und Dateiverschlüsselung).

Woher bekomme ich GPGTools?

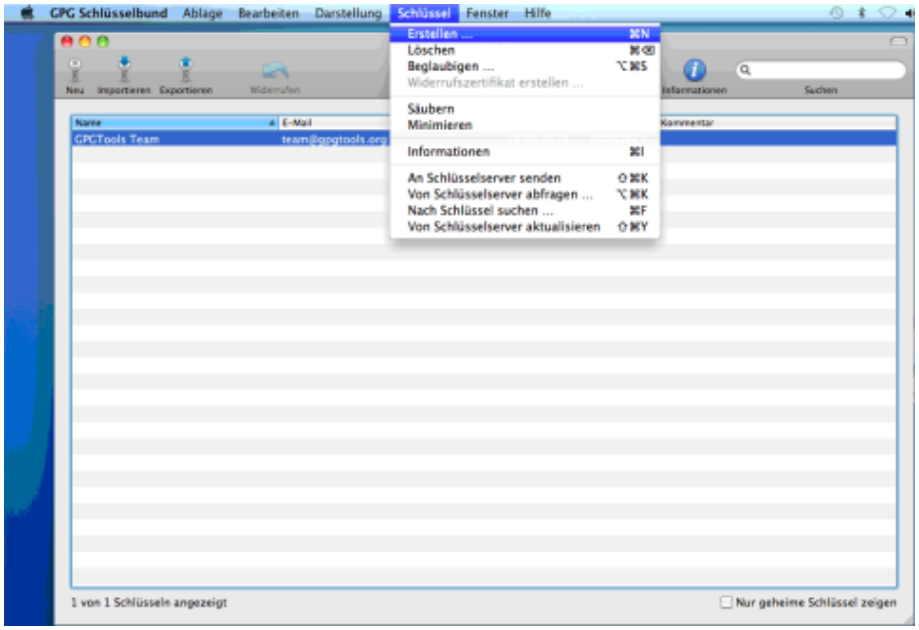
Alle o.g. Komponenten sind unter der Bezeichung GPGSuite unter folgender Adresse erhältlich: https://gpgtools.org/

I. Installation

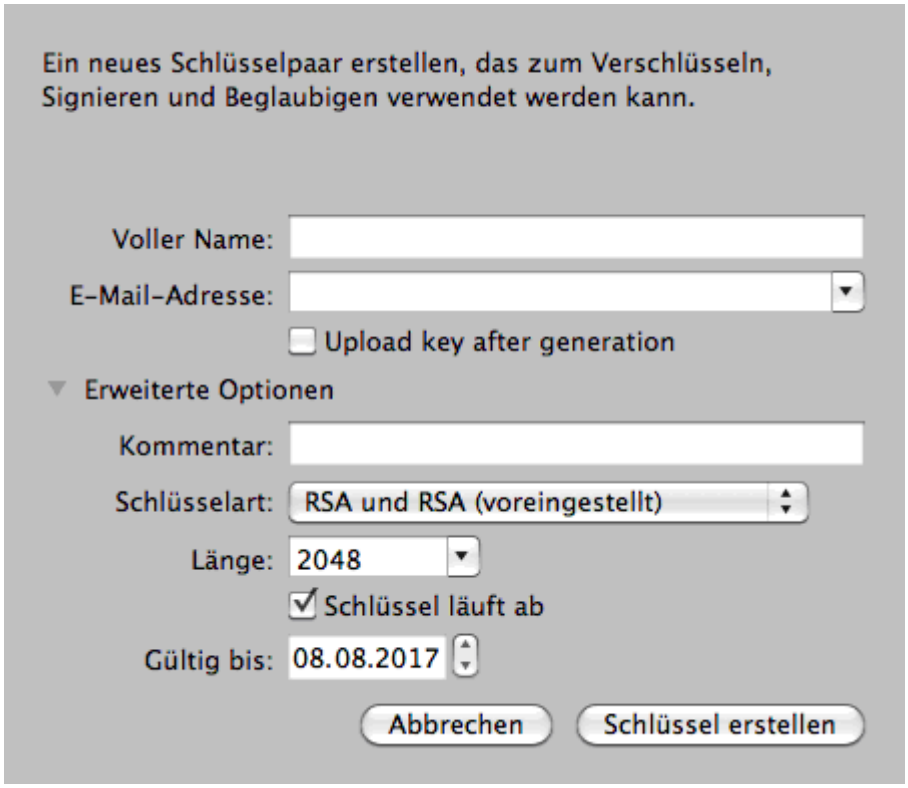
Nach dem Herunterladen steht das Installationsimage GPG Suite - JJJ.MM.TT.dmg im Downloadverzeichnis. Ein Doppelklick öffnet das Image, ein weiterer startet das Installationsprogramm (Administratorberechtigung erforderlich!). Sie werden Schritt für Schritt durch die Installation geführt.

II. Schlüsselpaar erzeugen

GPGTools nutzt eine Verfahren, das für die Ver- bzw. Entschlüsselung einem Schlüsselpaar aus einem öffentlichen und einem geheimen Schlüssel arbeitet. Sie brauchen also ein solches Schlüsselpaar. Sofern Sie noch kein Schlüsselpaar haben, müssen Sie eines erzeugen. Wenn sich der entsprechende Dialog nicht automatisch nach der Installation öffnet, starten Sie hierfür das Programm "GPG Keychain/GPG Schlüsselbund" in Ihrem Programmordner und wählen im Menü SCHLÜSSEL - ERSTELLEN.

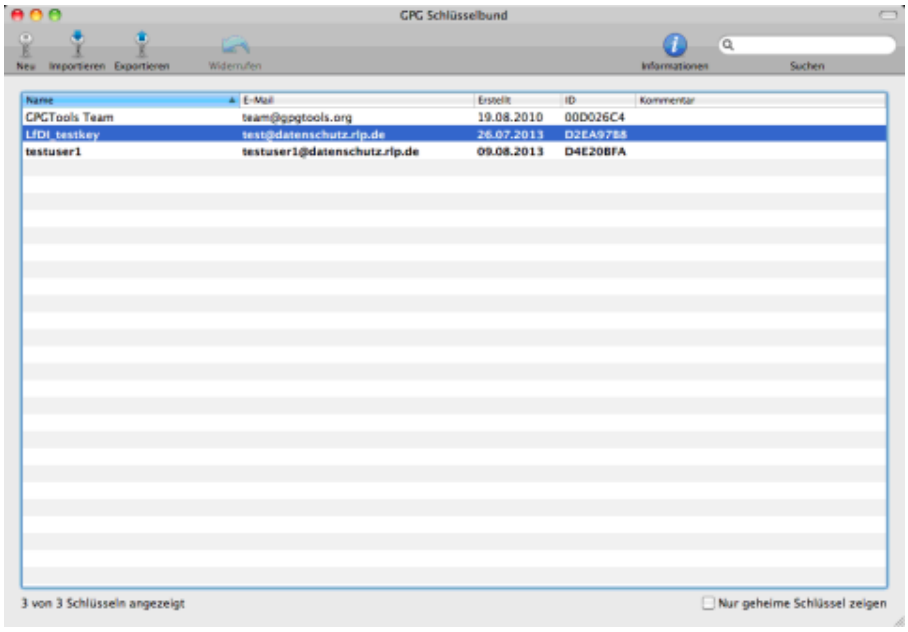


Wählen Sie einen Namen und eine E-Mail-Adresse. In den erweiterten Optionen kann man die Verschlüsselungsoptionen einstellen und ob es ein Ablaufdatum für die Gültigkeit des Schlüsselpaares geben soll (ein Verfallsdatum erhöht die Sicherheit, ist aber nicht zwingend notwendig).



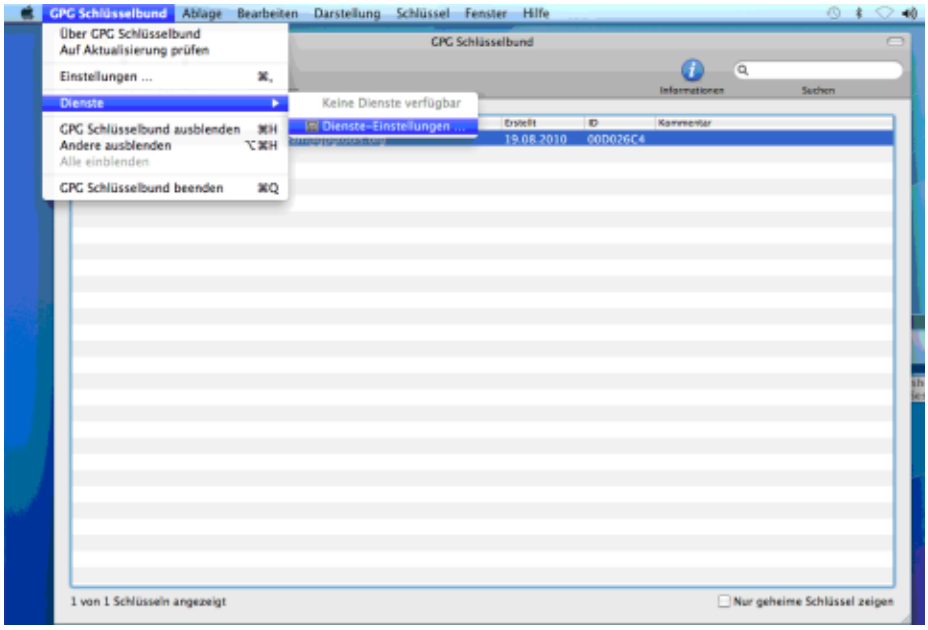
Dann müssen Sie noch eine "Passphrase" eingeben. Wählen Sie hierbei eine längere Zeichenfolge, die auch Ziffern oder Sonderzeichen enthält. Die Passphrase müssen Sie zur Sicherheit zwei Mail eingeben. Sie wird künftig immer abgefragt, wenn Sie den Schlüssel verwenden wollen.

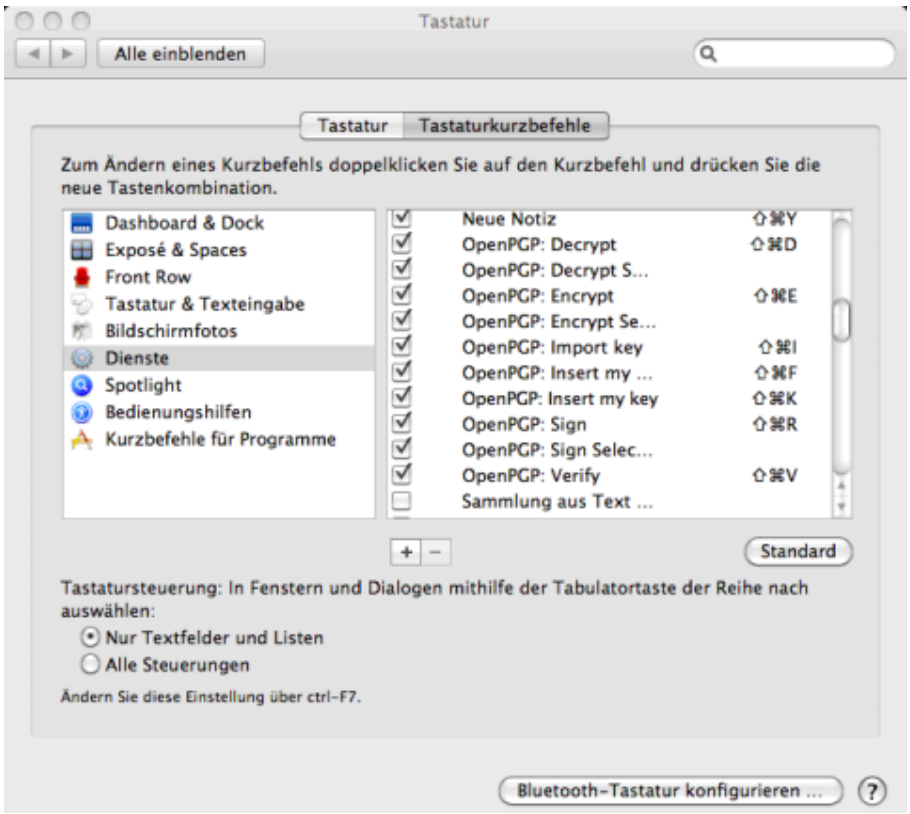
Wenn alles geklappt hat, erscheint Ihr Schlüssel in der Übersicht des GPG Schlüsselbunds.

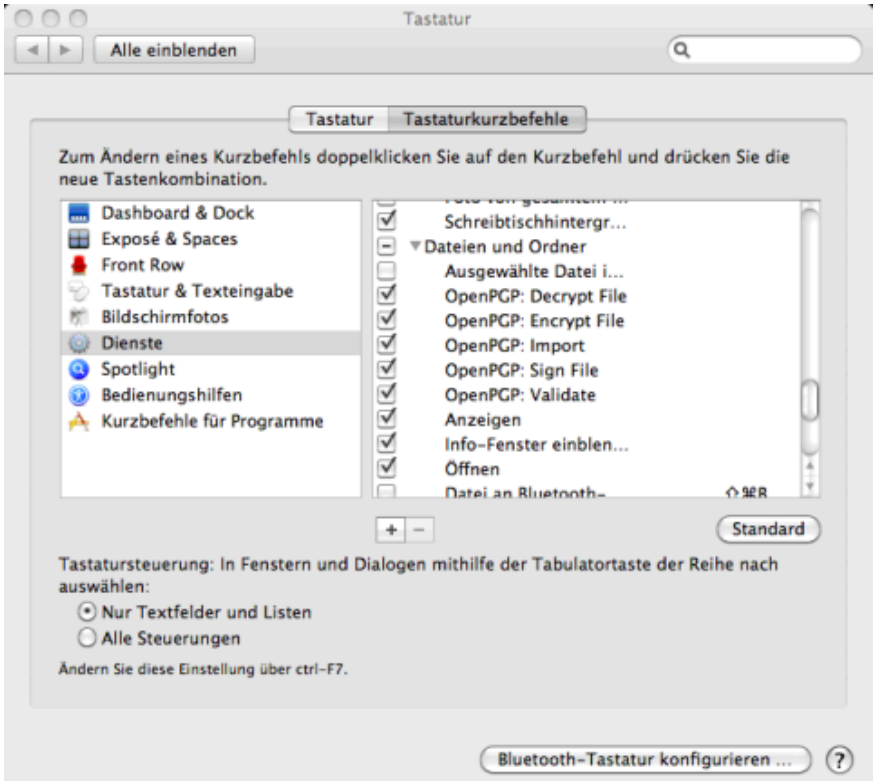


III. Dienste-Menü einstellen

Damit die Kryptofunktionen auch als Mac OSX-Dienste (z.B. im Kontextmenü via rechtem Mausklick) zur Verfügung stehen müssen Sie dies noch einstellen. Hierzu wählen Sie im Programm "GPG Schlüsselbund" im Menü die Punkte DIENSTE_DIENSTE-EINSTELLUNGEN und setzen dort in den Rubriken "Dateien und Ordner" und "Text" alle Häkchen bei den OpenPGP-Optionen.



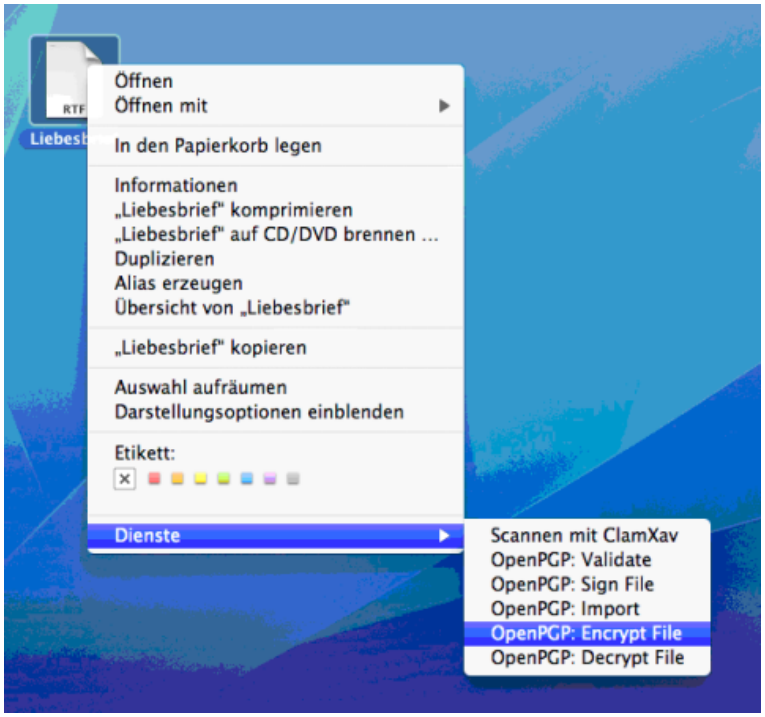




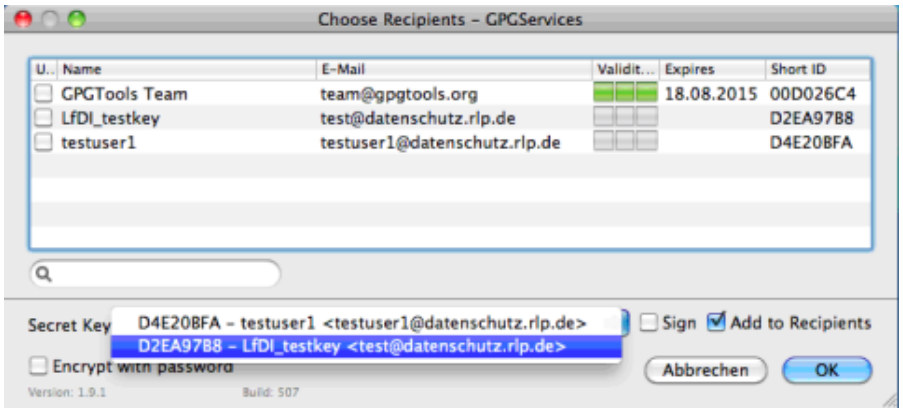
Damit können später Dateien oder markierter Text via rechtem Mausklick ver- bzw. entschlüsselt werden (siehe unten).

IV. Dateien verschlüsseln

Um einzelne Dateien zu verschlüsseln und sie als Anlage einer Mail beizufügen, gehen Sie wie folgt vor: Wählen Sie die die zu verschlüsselnde Datei (im Beispiel: "Liebesbrief.odt") mit einem Linksklick aus und rufen anschließend mit einem Rechtsklick das Kontextmenu auf. Wählen Sie hier den Menüpunkt "Dienste" und danach "OpenPGP Encrypt File".



Wählen Sie danach dem Empfänger aus, für den Sie die Datei verschlüsseln möchten.



Anmerkung: Sie benötigen von jedem Empfänger, dem Sie die verschlüsselte Datei zukommen lassen wollen, den "öffentlichen GnuPG-Schlüssel". Um sicherzustellen, dass Sie das Chiffrat ggf. auch selbst wieder öffnen können, sollte der öffentliche Schlüssel des Absenders ebenfalls eingebunden werden.

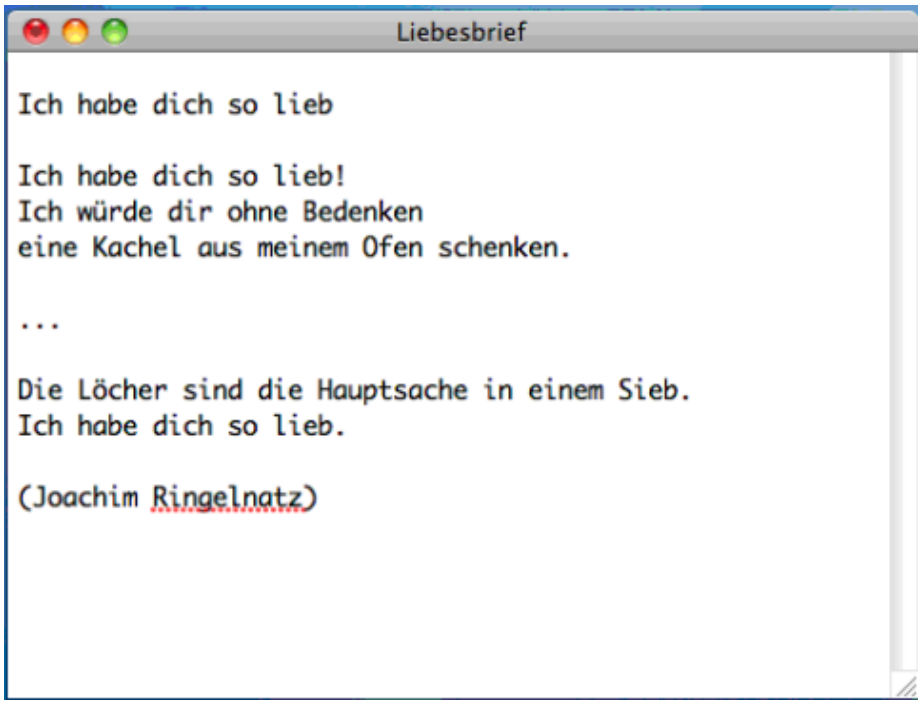
Wenn alles geklappt hat, wird es Ihnen angezeigt.

Die verschlüsselte Datei - das so genannte Chiffrat - befindet sich im gleichen Ordner wie die Ausgangsdatei. Sie trägt den gleichen Namen und hat die Namenserweiterung ".gpg". Diese Datei können Sie jetzt z.B. per Mail verschicken.

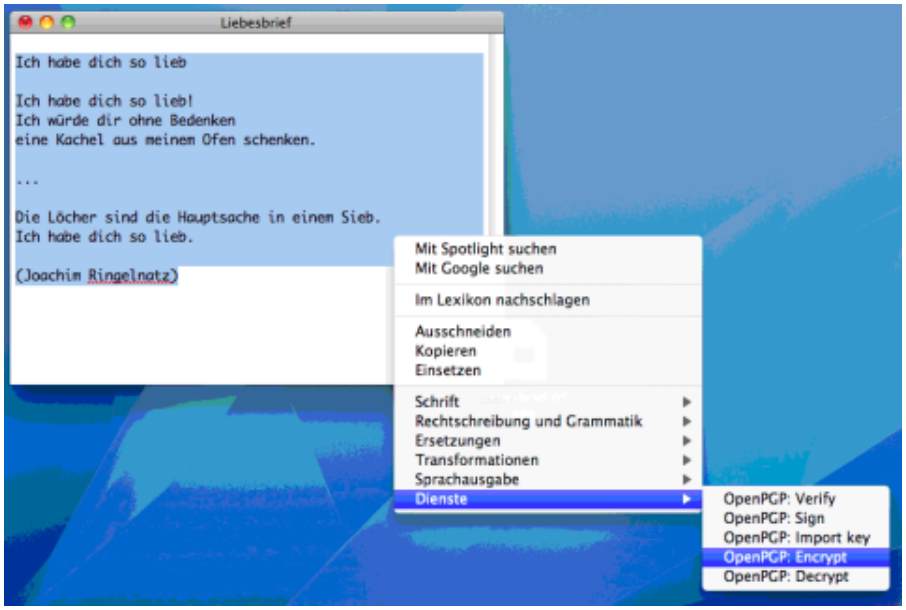
V. Verschlüsseln von Texten über die Zwischenablage

Statt einzelne Dateien zu verschlüsseln und diese als Anlage einer E-Mail bezufügen, können Sie Texte auch über die Zwischenablage verschlüsseln.

Angenommen, dies ist der Text, den Sie verschlüsseln möchten. Gehen Sie folgendermaßen vor:

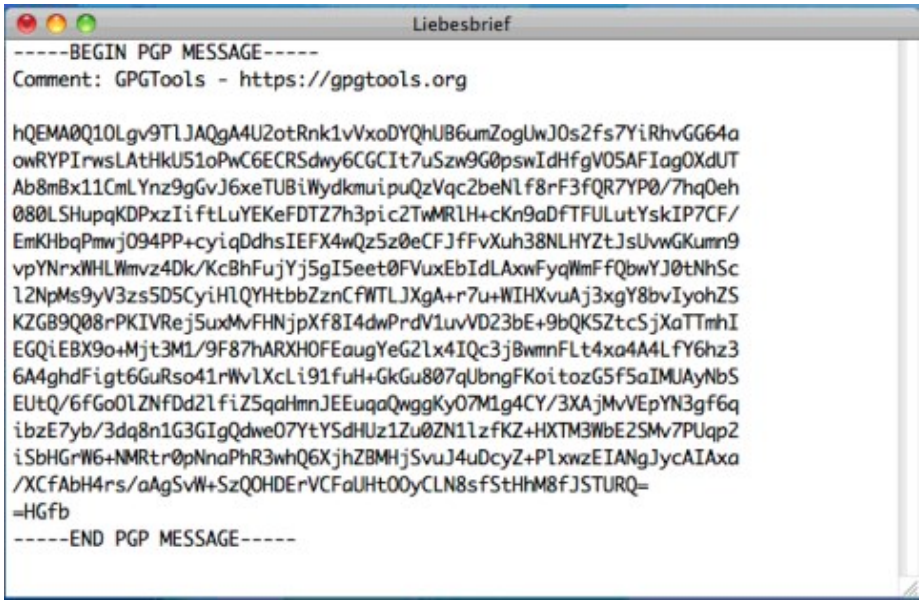


Markieren Sie den zu verschlüsselnden Text, rufen Sie mit einem Rechtsklick das Kontextmenü auf und wählen Sie "Dienste" und "OpenPGP Encrypt":



Wählen Sie im folgenden Dialog einen Empfänger aus. Auch hier benötigen Sie den öffentlichen GnuPG-Schlüssel desjenigen, dem Sie die verschlüsselte Nachricht zukommen lassen wollen.

Der verschlüsselte Text wird eingesetzt und ersetzt den ursprünglichen Text. Er ist eingschlossen in die Begriffe "---- Beginn PGP Message---- und "----End PGP Message----". Per Zwischenablage kann dieser z.B. in eine E-Mail übernommen werden.



VI. Entschlüsseln

Das Entschlüsseln von Dateien oder von Texten in der Zwischenablage erfolgt in gleicher Weise, nur wählen Sie hier den Menüpunkt "OpenPGP Decrypt".

Weitere Informationen zum Einstieg in GPGTools stehen in der GPGTools Knowledge Base (englisch):

- http://support.gpgtools.org/kb/how-to/first-steps-where-do-i-start-where-do-i-begin

oder hier:

- http://www.verbraucher-sicher-online.de/anleitung/bildfolge-verschluesseln-mit-gpgtools-mac-os-x-die-gpg-suite-installieren

VII. Hinweis

Das GNUPG-Verfahren funktioniert plattformübergreifend. Das heißt mit entsprechenden Programmen für Windows, iPad/iPhone (iOS) oder Android-Geräte können Sie auch dort Dateien oder Texte bearbeiten. Dies sind z.B.:

- für Windows Computer das kostenlose Programmpaket GPG4Win
- für iPad und iPhone (iOS)
    - das kostenlose Programm "OpenGP Lite" aus dem App-Store.
- für Android Tabelts und Smartphones
    - das kostenlose Programm APG aus dem Google Play Store