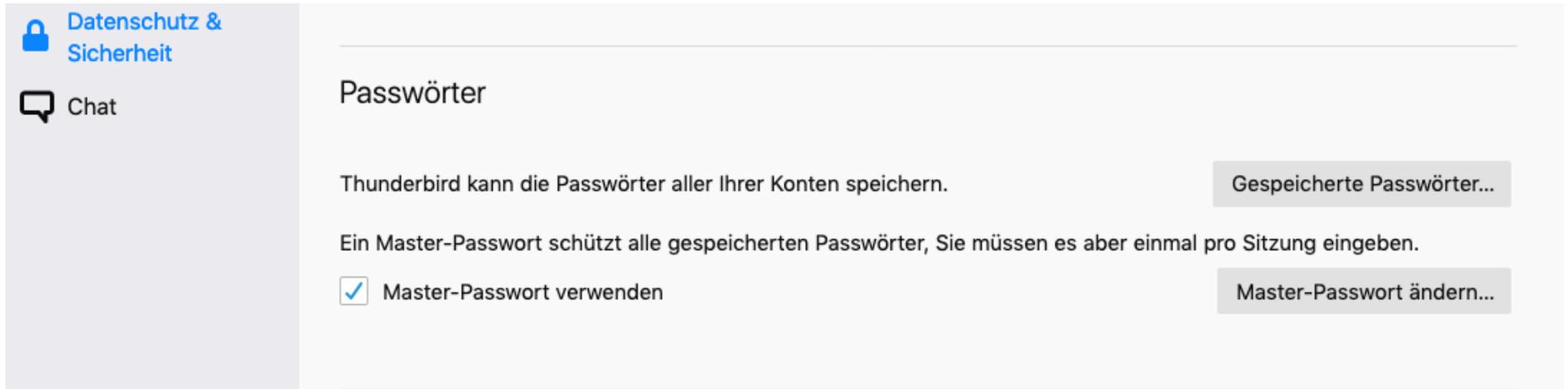


E-Mail-Verschlüsselung im E-Mail-Client Thunderbird ab Version 78 Praktische Durchführung

Vorbemerkung:

Der E-Mail-Client Thunderbird hat als quelloffenes nichtkommerzielles Programm seit Version 78 die Verschlüsselungswerkzeuge schon integriert

1) In „Einstellungen,, von Thunderbird ein Master-Passwort vergeben und gut merken bzw. sicher verwahren.
Dieses dient später dem Schutz und der bedarfsweisen Nutzung des Privaten PGP-Schlüssels, solange das Programm Thunderbird geöffnet ist.
Nur dieses Master-Passwort erschließt den Zugang zu verschlüsselten E-Mails.



The screenshot shows the 'Datenschutz & Sicherheit' (Data Protection & Security) settings page in Thunderbird. The left sidebar contains a lock icon for 'Datenschutz & Sicherheit' and a chat icon for 'Chat'. The main content area is titled 'Passwörter' (Passwords). It contains the following text: 'Thunderbird kann die Passwörter aller Ihrer Konten speichern.' (Thunderbird can save the passwords of all your accounts.) followed by a button 'Gespeicherte Passwörter...' (Saved passwords...). Below this, it says 'Ein Master-Passwort schützt alle gespeicherten Passwörter, Sie müssen es aber einmal pro Sitzung eingeben.' (A master password protects all saved passwords, but you must enter it once per session.) At the bottom, there is a checked checkbox 'Master-Passwort verwenden' (Use master password) and a button 'Master-Passwort ändern...' (Change master password...).

Datenschutz & Sicherheit

Chat

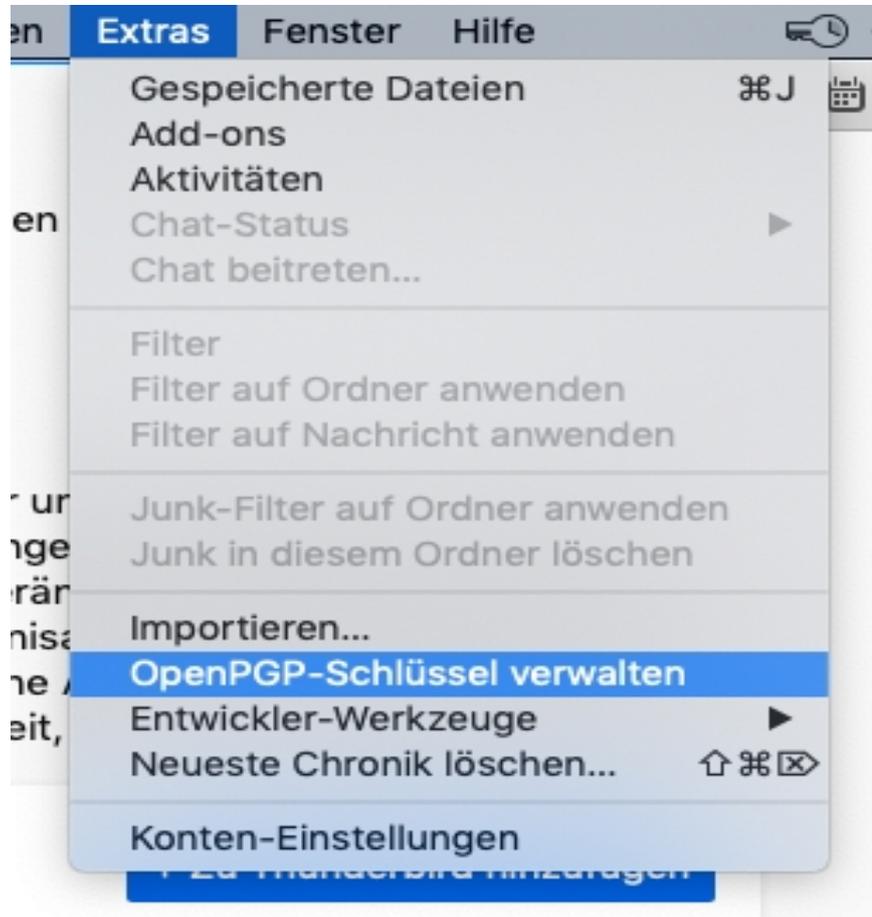
Passwörter

Thunderbird kann die Passwörter aller Ihrer Konten speichern. [Gespeicherte Passwörter...](#)

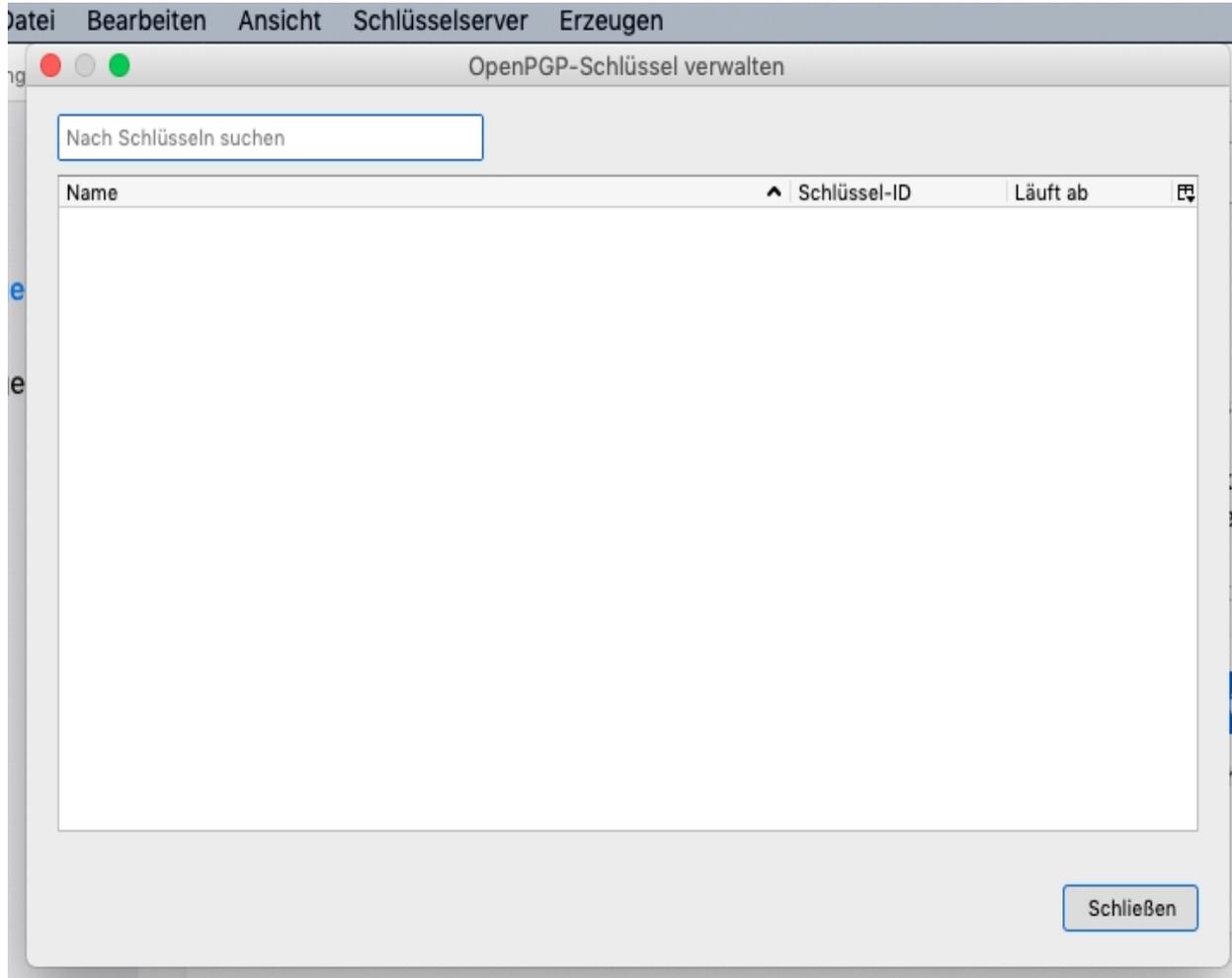
Ein Master-Passwort schützt alle gespeicherten Passwörter, Sie müssen es aber einmal pro Sitzung eingeben.

Master-Passwort verwenden [Master-Passwort ändern...](#)

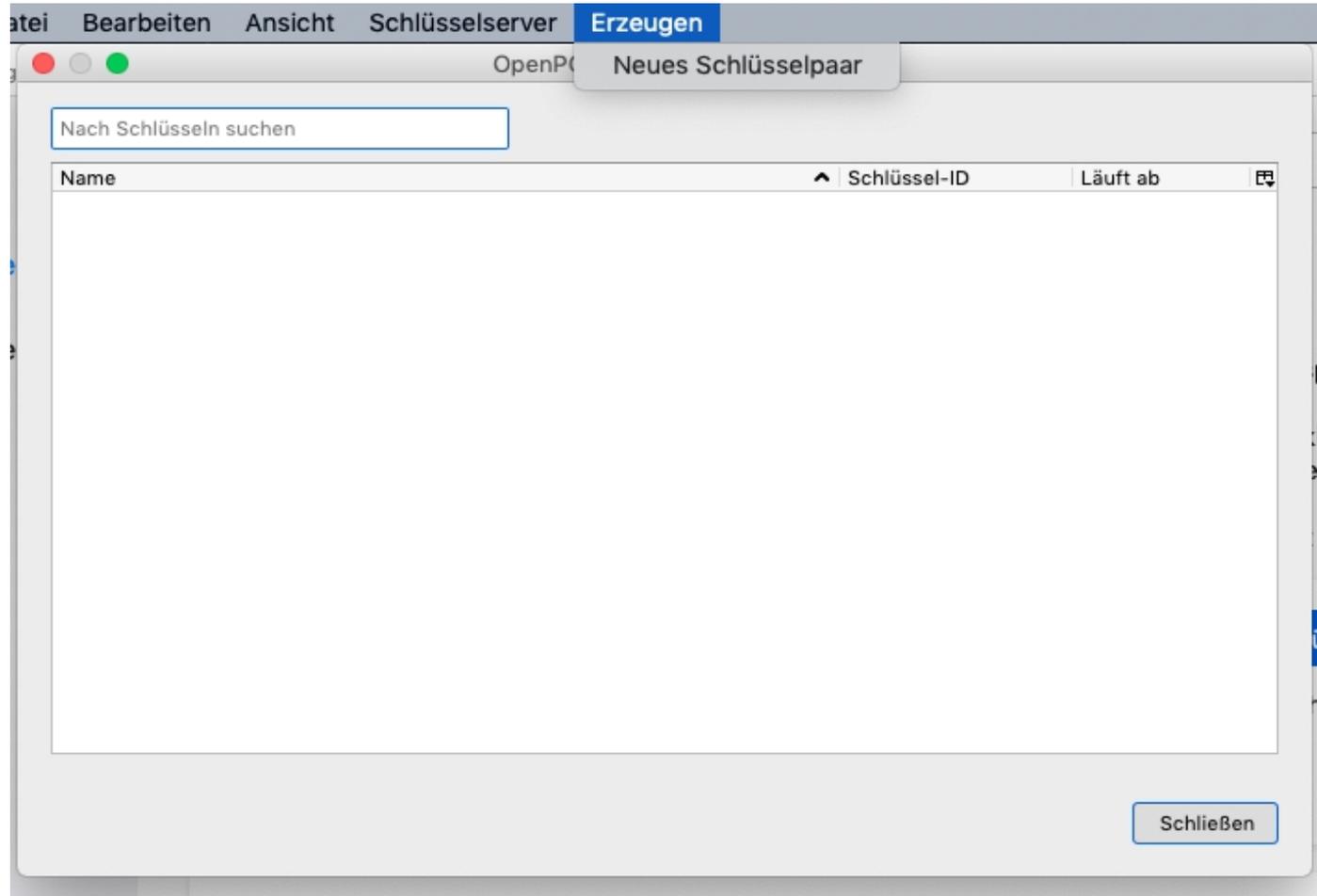
2) Bei geöffnetem Programm Thunderbird unter „Extras“ den Menü-Punkt „Open-PGP-Schlüssel verwalten“ aufrufen



Man sieht zunächst ein leeres Formular, den noch leeren Schlüsselbund.



3) Unter „Erzeugen“ kann jetzt das eigene Schlüsselpaar (privater mit öffentlichem Schlüssel) erzeugt werden. „Neues Schlüsselpaar“



4) Man legt dabei zunächst die Identität fest, d.h. die Zugehörigkeit zur

- E-Mail-Adresse
- Ablaufdatum des Schlüssels (Gültigkeitsdauer)
- Schlüsseltyp: RSA
- Schlüsselgröße: 4096

OpenPGP-Schlüssel erzeugen

Nach Schließen

Name

Identität Ulrich Boesenecker <ulib@posteo.de> - ulib@posteo.de

Ablaufdatum

Legen Sie das Ablaufdatum Ihres neu erzeugten Schlüssels fest. Sie können das Datum später weiter in die Zukunft verschieben, falls nötig.

Schlüssel läuft ab in 10 Tagen

Schlüssel läuft nicht ab

Erweiterte Einstellungen

Erweiterte Einstellungen für Ihren OpenPGP-Schlüssel festlegen

Schlüsseltyp: RSA

Schlüsselgröße: 4096

?

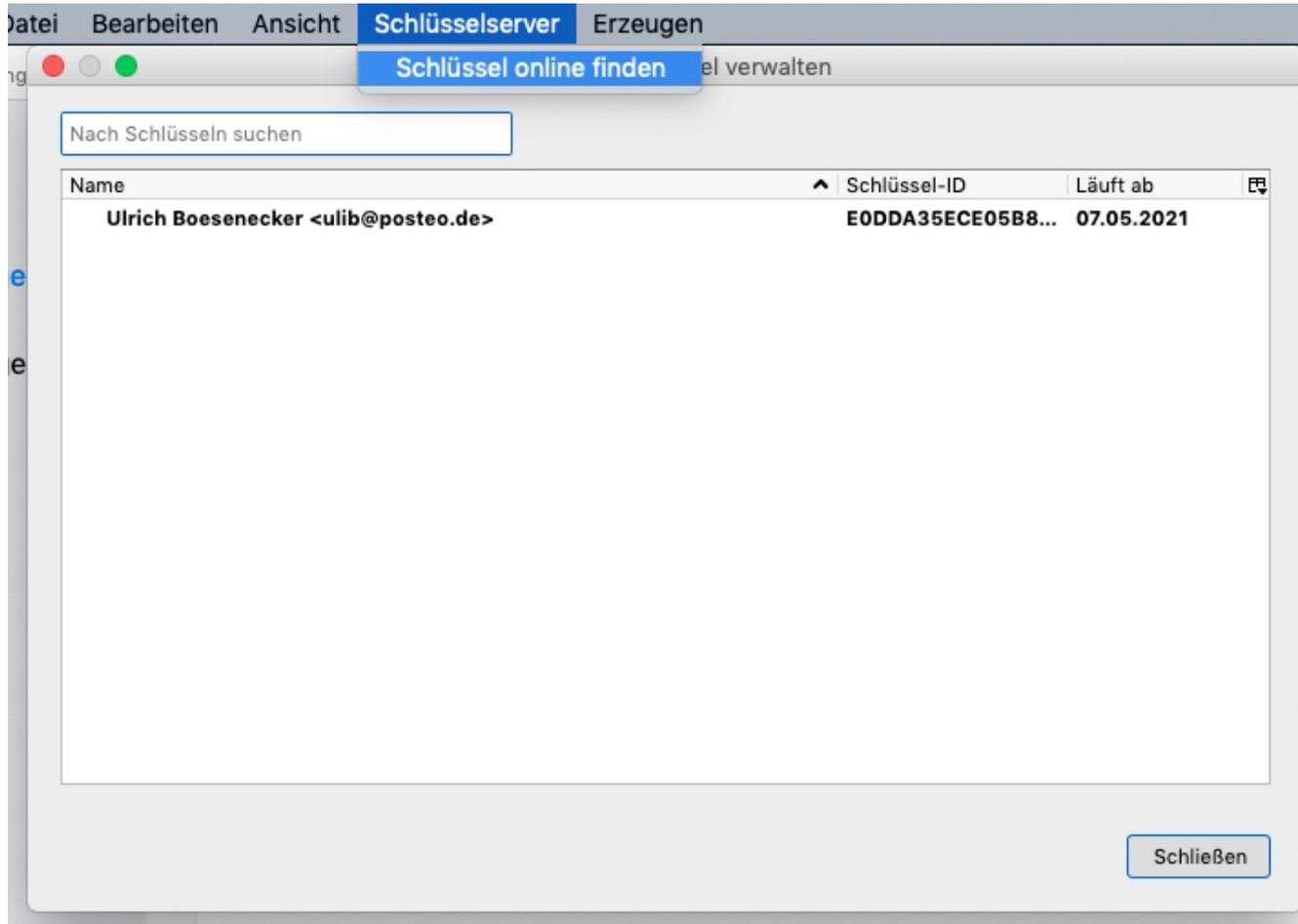
Abbrechen Schlüssel erzeugen

Schließen

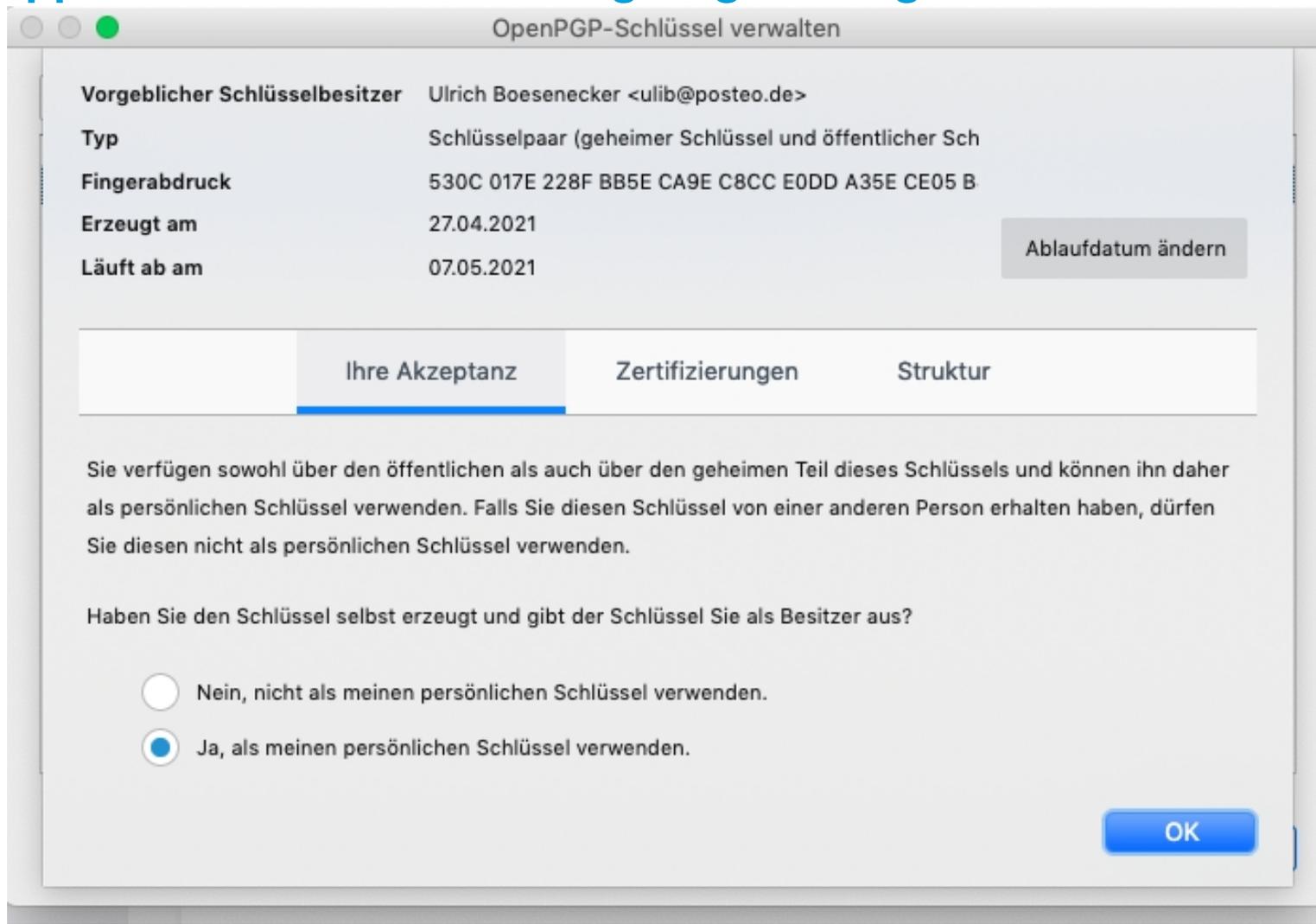
Mausbewegungen oder offene weitere Programme wie Browser / Video während der Sekunden der zufälligen Berechnung verbessern die Schlüsselqualität.



5) Anschließend ist der persönliche PGP-Schlüssel
(privat+öffentlich in Fettschrift!)
im zuvor leeren Schlüsselbund zu sehen.

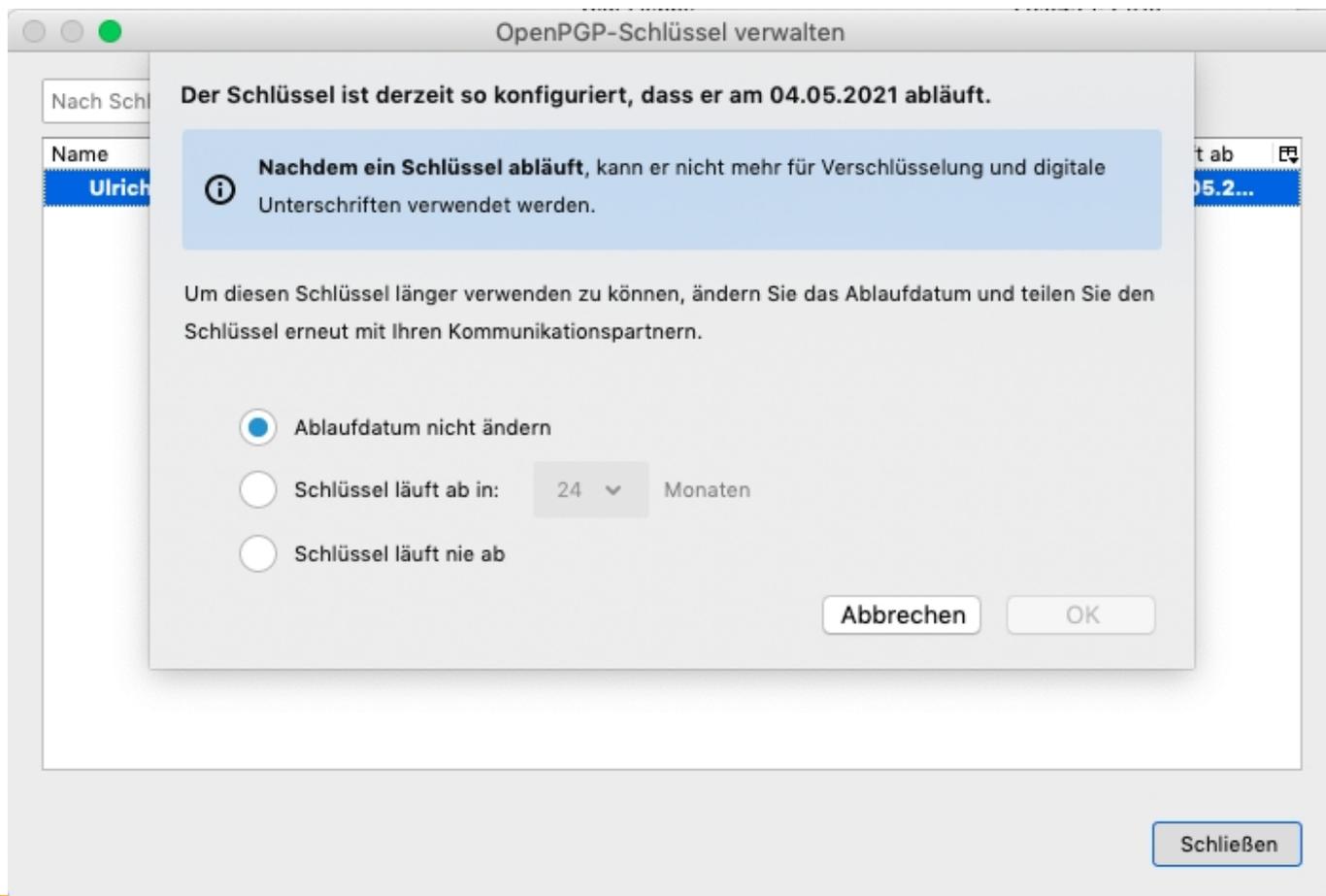


6) Doppelklick auf diesen Eintrag zeigt die Eigenschaften im Einzelnen.

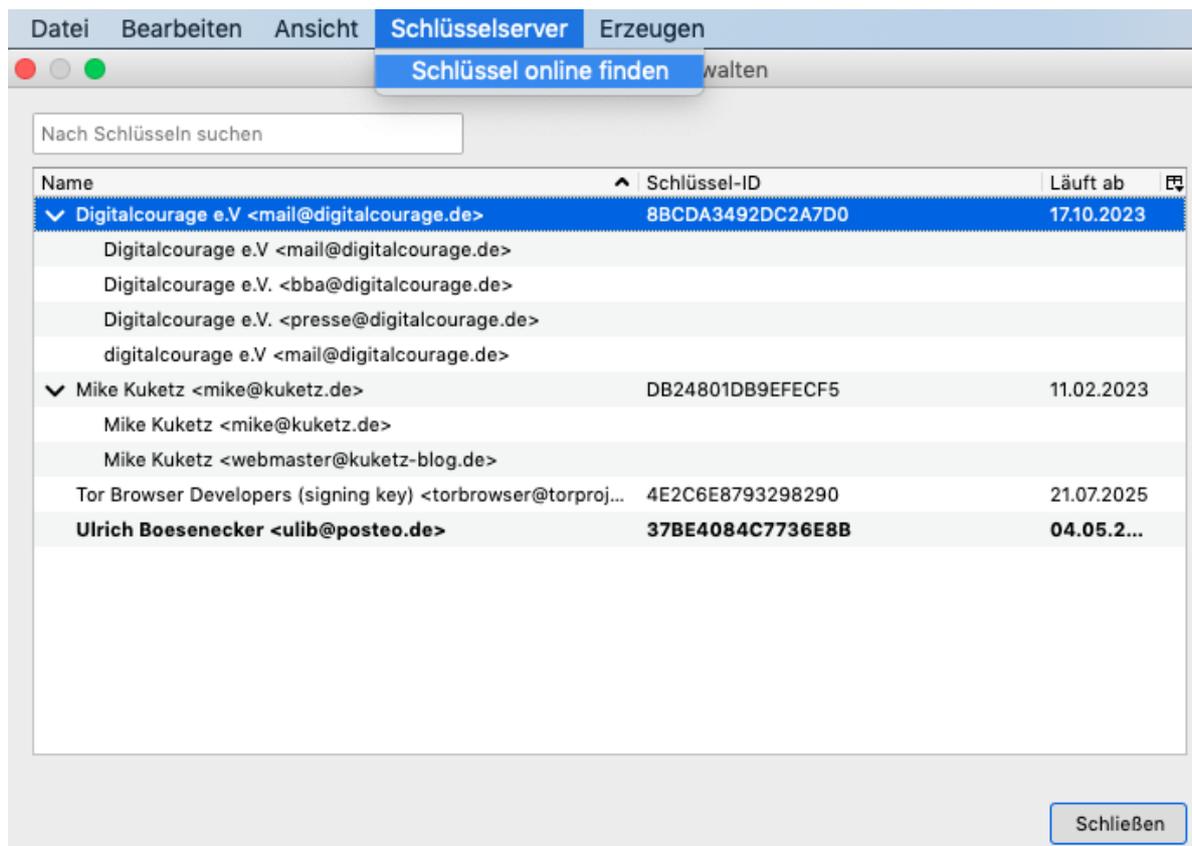


> Markierung setzen bei: „Ja, als meinen persönlichen Schlüssel verwenden.“

In diesem Formular kann auch später noch das Ablaufdatum geändert bzw. verlängert werden, sogar wenn das Ablaufdatum überschritten ist.



7) Unter dem Punkt „Schlüsselserver“ können mit „Schlüssel online finden“ ggf. verschlüsselungsfähige Kommunikationspartner über ihre E-Mailadresse gefunden und deren öffentliche Schlüssel vom Schlüsselserver auf den eigenen Rechner in den Schlüsselbund heruntergeladen werden. Sie erscheinen dort nicht in Fettschrift. Mehrere Adressen können mit einem Schlüssel verbunden sein.



8) Der unterste Menüpunkt unter „Extras“ in Thunderbird ist „Konten-Einstellungen“

mit dem Unterpunkt „Ende-zu-Ende-Verschlüsselung“

Wir wählen hier nicht S/MIME das eher verbreitet ist im geschäftlichen Bereich mit oft kostenpflichtigen Zertifikaten, sondern OpenPGP mit dem persönlichen zuvor erzeugten Schlüssel aus.

„Keiner“ läßt eine getroffene Vorauswahl im Fall erneuter Erzeugung eines persönlichen Schlüsselpaars nachträglich korrigieren

Thunderbird Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Extras Fenster Hilfe

Posteingang Thunderbird Privac... Add-ons-Verwaltun... Einstellungen

ulib@posteo.de

- Server-Einstellungen
- Kopien & Ordner
- Verfassen & Adressieren
- Junk-Filter
- Synchronisation & Speicherplatz
- Ende-zu-Ende-Verschlüsselung**
- Empfangsbestätigungen (MDN)

Lokale Ordner

- Junk-Filter
- Speicherplatz

Postausgangs-Server (SMTP)

Ende-zu-Ende-Verschlüsselung

Um Nachrichten zu verschlüsseln oder zu entschlüsseln, benötigen Sie eine Verschlüsselungstechnologie. OpenPGP ist eine weit verbreitete Technologie zur Verschlüsselung von E-Mails.

Wählen Sie Ihren persönlichen Schlüssel für S/MIME. Falls Sie kein persönliches Zertifikat für S/MIME. Falls Sie kein persönliches Zertifikat verfügen Sie über einen persönlichen Schlüssel. [Weitere Informationen](#)

OpenPGP

Thunderbird verfügt über 1 persönlichen OpenPGP-Schlüssel für **ulib@posteo.de**.

 ✓ Derzeit ist die Verwendung der Schlüssel-ID **0xE0DDA35ECE05B8D0** festgelegt. [Weitere Informationen](#)

[Schlüssel hinzufügen...](#)

Keiner

OpenPGP für diese Identität nicht verwenden

0xE0DDA35ECE05B8D0

Der Schlüssel läuft nicht ab.

Extras Menü:

- Gespeicherte Dateien
- Add-ons
- Aktivitäten
- Chat-Status
- Chat beitreten...
- Filter
- Filter auf Ordner anwenden
- Filter auf Nachricht anwenden
- Junk-Filter auf Ordner anwenden
- Junk in diesem Ordner löschen
- Importieren...
- OpenPGP-Schlüssel verwalten
- Entwickler-Werkzeuge
- Neueste Chronik löschen...
- Konten-Einstellungen**

9) Nach einmaliger, später veränderbarer Einstellung der Sende-Vorgaben unter **Konto-Einstellungen/Ende-zu-Ende-Verschlüsselung** (im Fenster ganz nach unten scrollen) kann man an Verschlüsselungs-Kommunikationspartner eine signierte und verschlüsselte Mail versenden.

Ende-zu-Ende-Verschlüsselung

Empfangsbestätigungen (MDN)

▼ Lokale Ordner

Junk-Filter

Speicherplatz

Postausgangs-Server (SMTP)

Senden von Nachrichten - Standardeinstellungen

Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-Mail-Anbieter leicht zugänglich und kann auch Bestandteil einer Massenüberwachung werden.

- Verschlüsselung standardmäßig nicht aktivieren
- Verschlüsselung standardmäßig verlangen

Falls Sie Verschlüsselung verwenden, benötigen Sie zum Senden einer Nachricht für jeden Empfänger dessen öffentlichen Schlüssel oder das Zertifikat.

Eine digitale Unterschrift ermöglicht den Empfängern zu überprüfen, dass die Nachricht von Ihnen gesendet sowie der Inhalt nicht geändert wurde.

- Eigene digitale Unterschrift standardmäßig hinzufügen

Verschlüsselung und Signatur ist im Empfänger-Thunderbird an den Symbolen rechts oben erkennbar.

Von Ulrich Boesenecker 

Betreff **Test**

An Ulrich Boesenecker 

 Antworten

 Weiterleiten

 Archivieren

 Junk

 Löschen

Mehr 

15:26

OpenPGP  

Verschlüsselter und signierter E-Mail-Text

Nachrichten-Sicherheit - OpenPGP

Gute digitale Unterschrift

Diese Nachricht enthält eine gültige digitale Unterschrift mit Ihrem persönlichen Schlüssel.

Schlüssel-ID der digitalen Unterschrift:
0x37BE4084C7736E8B

Schlüssel der digitalen Unterschrift anzeigen

Nachricht ist verschlüsselt

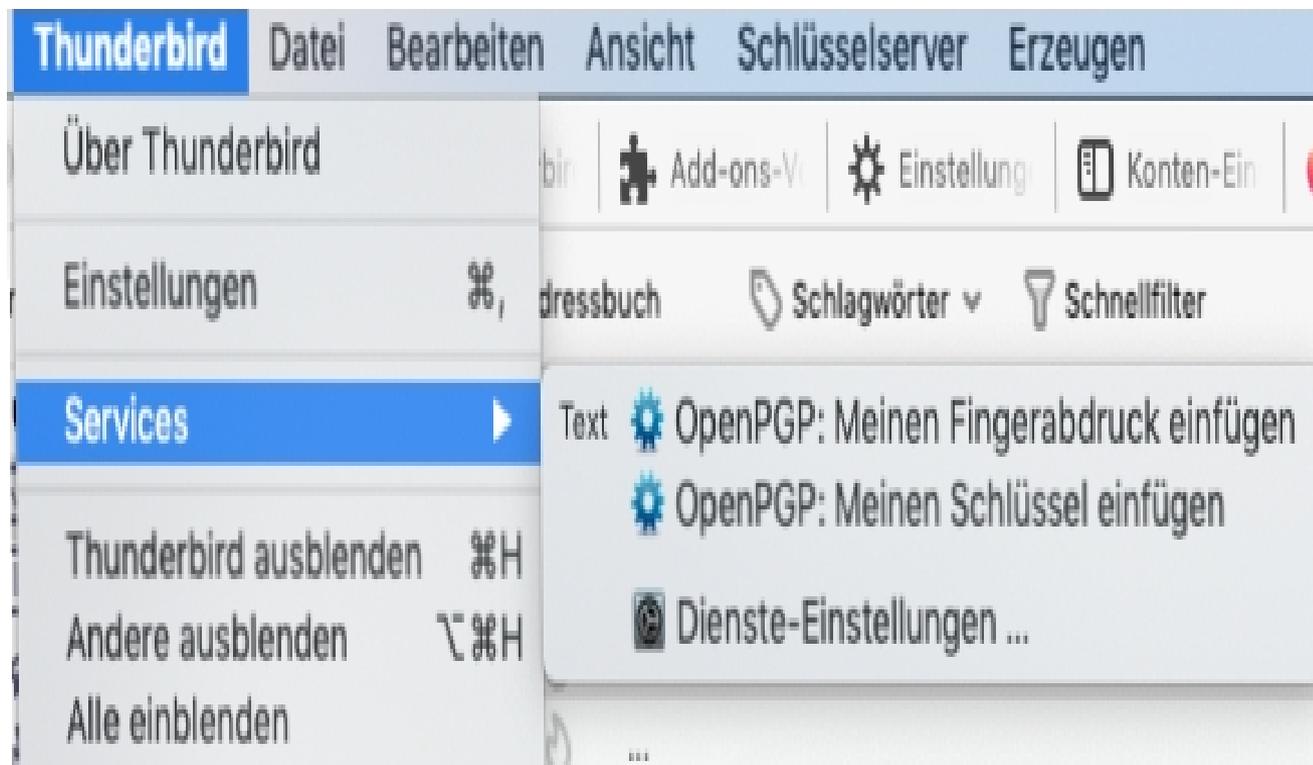
Diese Nachricht wurde verschlüsselt, bevor sie an Sie gesendet wurde. Die Verschlüsselung macht es sehr schwierig für andere Personen, Ihre Informationen während der Übertragung über das Netzwerk / Internet anzusehen.

Ihre Schlüssel-ID für Entschlüsselung: 0x37BE4084C7736E8B
(Unterschlüssel-ID: 0xF6FDB58B3CFB7A35)

Ihren Schlüssel für Entschlüsselung anzeigen

>  1 Anhang: OpenPGP_0x37BE4084C7736E8B.asc 3.1 KB

Auch kann der eigene öffentliche Schlüssel für die Rückantwort und für den Schlüsselbund des Empfängers mitsamt dem „Fingerabdruck“ automatisch dabei mitgesendet werden.

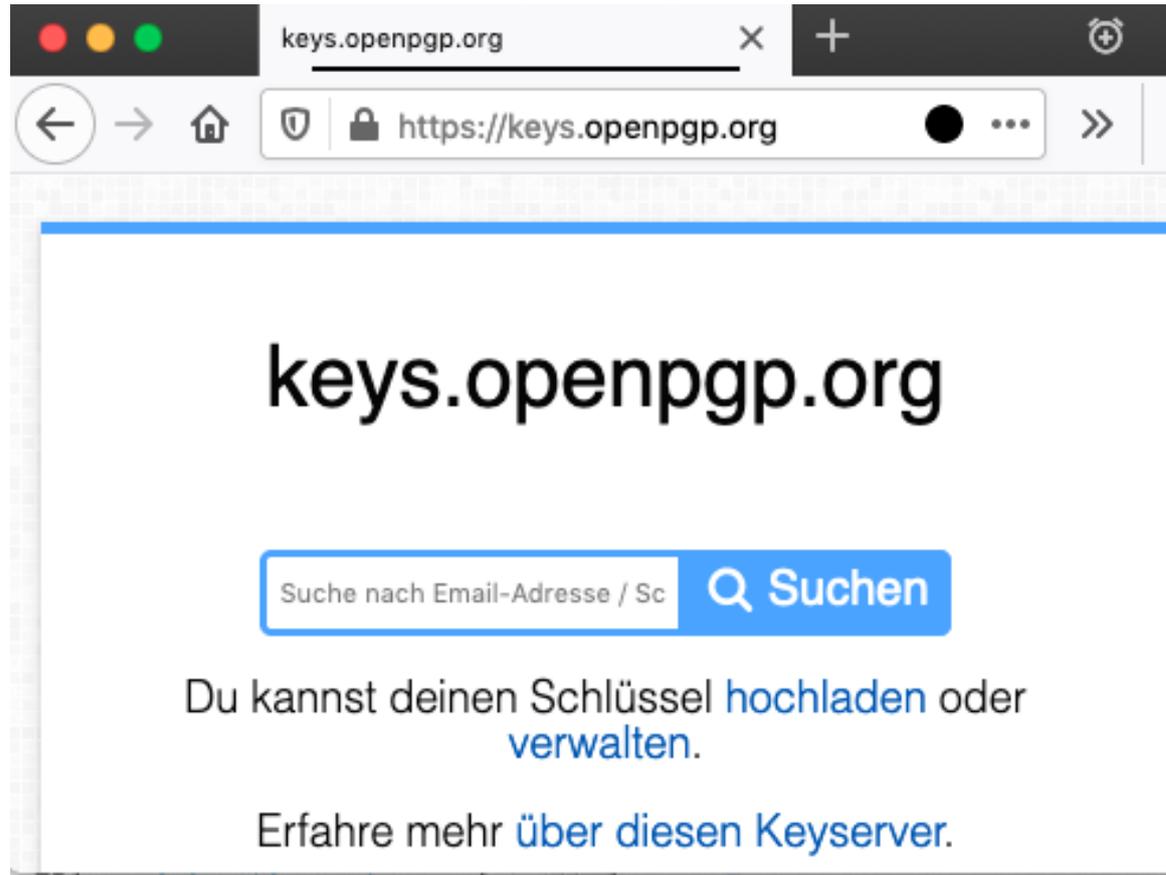


Keine Sorge!

„Nichtverschlüssler“

werden ganz normal von unverschlüsselten E-Mails erreicht.

10) Eine weitere Schlüssel-Verteilermethode geht über einen Schlüsselservers: Unter keys.openpgp.org können im Browser wie Firefox nicht nur E-Mail-Adressen mit Schlüssel-Zuordnung gefunden werden, sondern auch der eigene öffentliche PGP-Schlüssel hochgeladen und per Bestätigungsmail für andere Nutzer als eindeutig zur wahren Mail-Adresse gehörig verifiziert werden.



Fragen?