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

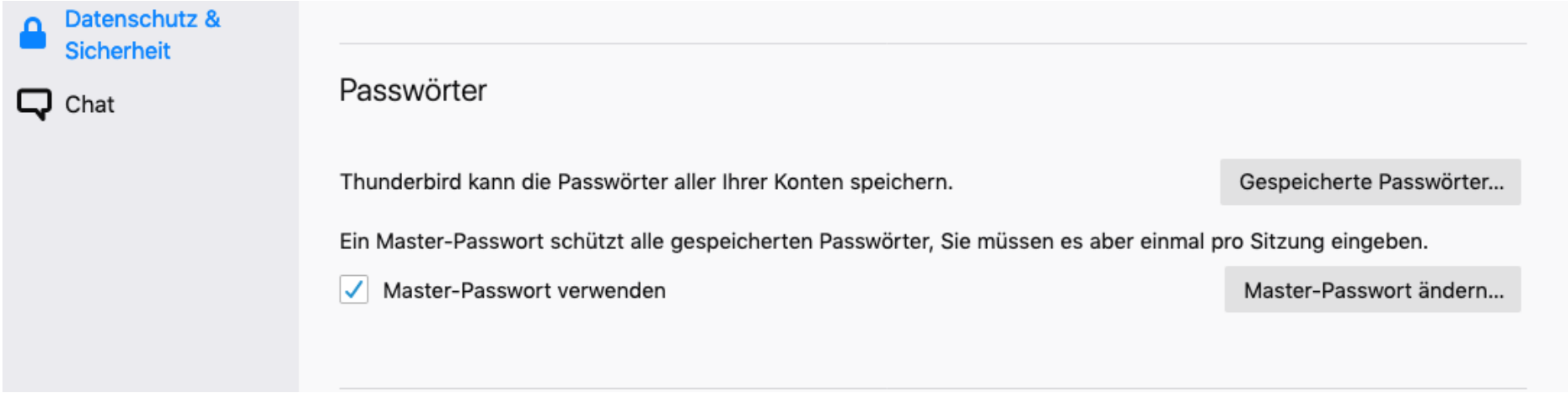
Uli Boesenecker - Cryptoparty Tübingen - April 2022 https://cryptoparty-tuebingen.de/

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

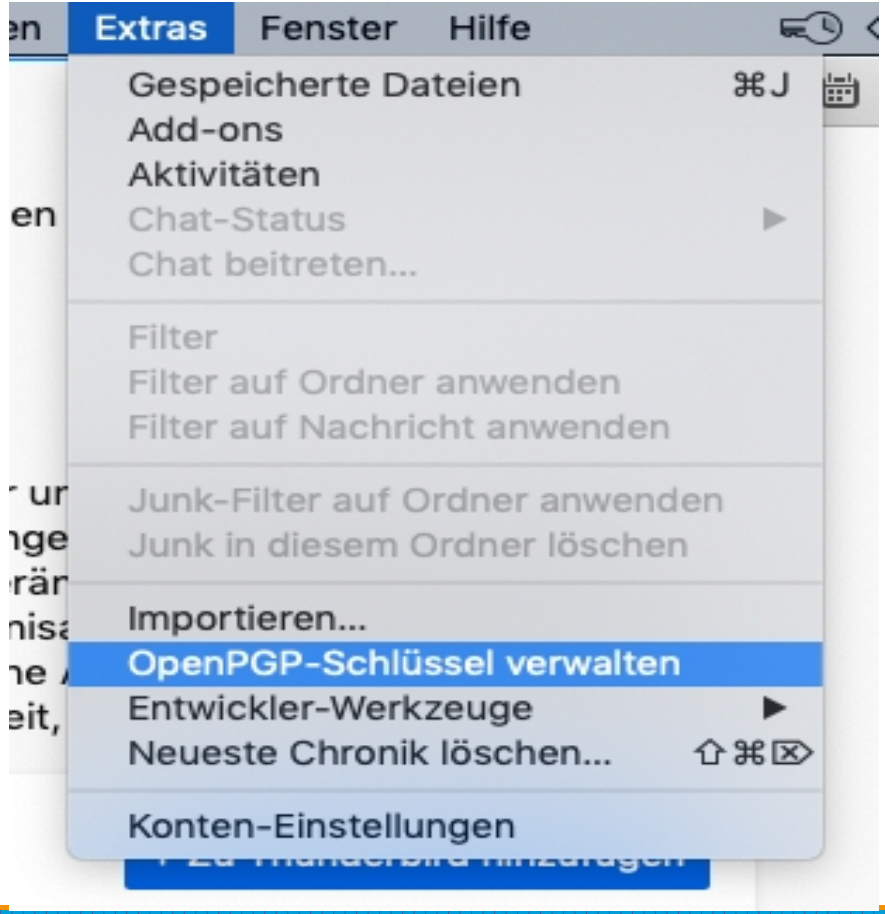
Vorliegende Präsentation wurde mit der Mac-Version von Thunderbird erstellt.

Die Optik auf anderen Betriebssystemen kann leicht abweichen.

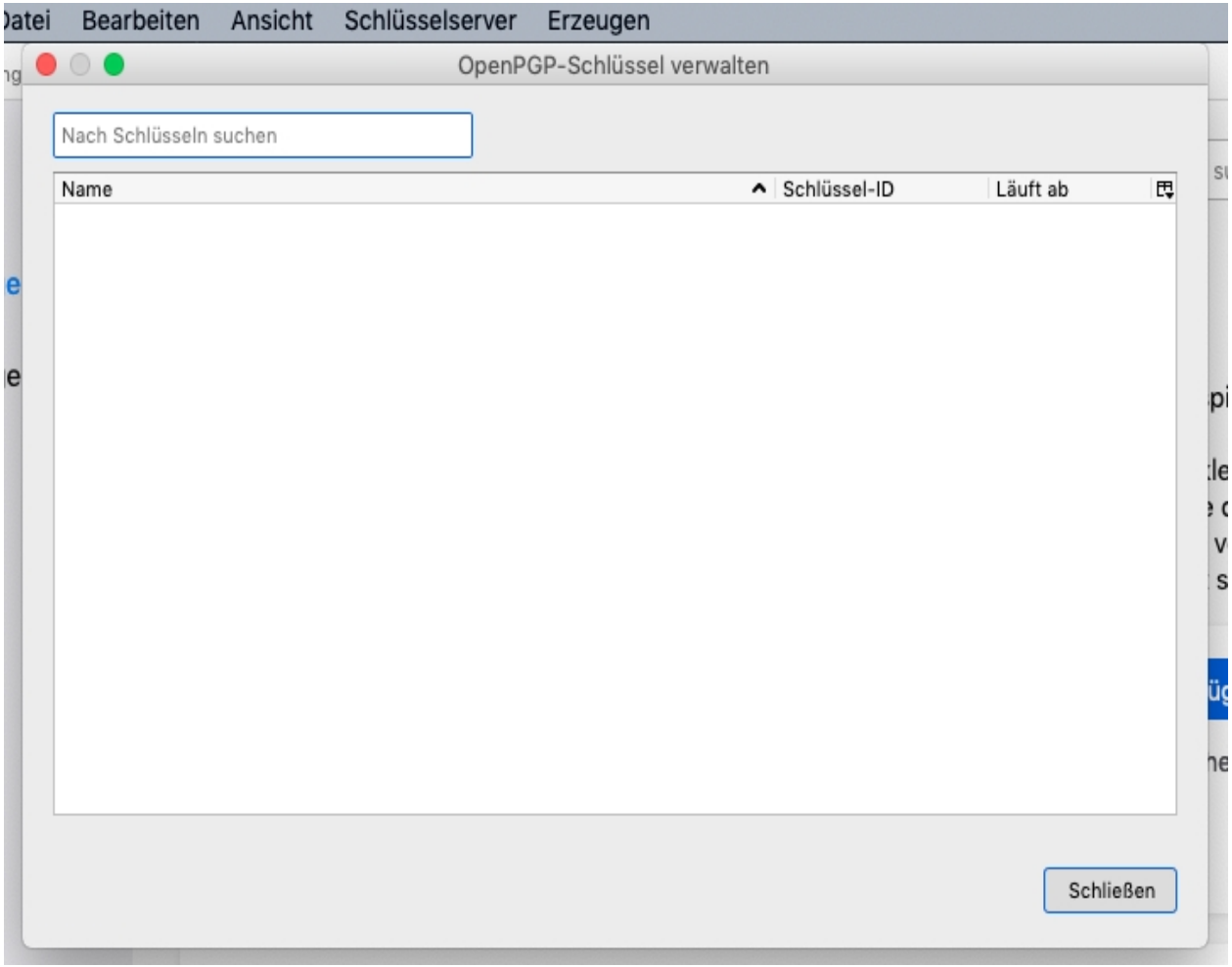
1) In „Einstellungen/ Datenschutz + Sicherheit“ von Thunderbird ein Master-Passwort vergeben und gut merken bzw. sicher verwahren. Dieses dient später dem Schutz und der bedarfsweisen Nutzung des Privaten PGP-Schlüssels, solange das Programm Thunderbird geöffnet ist. Nur dieses Master-Passwort erschließt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



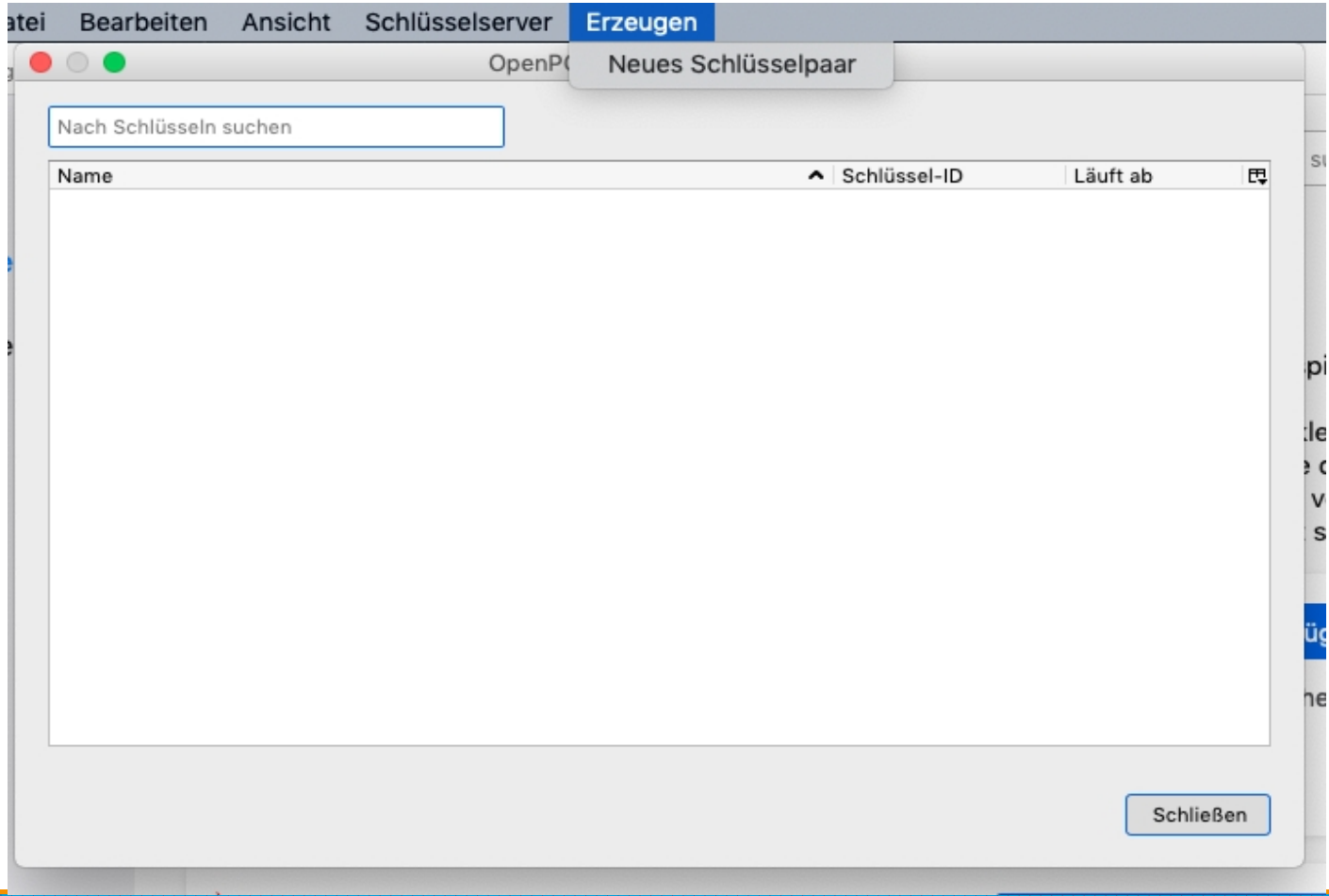
2) Bei geöffnetem Programm Thunderbird unter „Extras“ den Menü-Punkt „Open-PGP-Schlüssel verwalten“ aufrufen



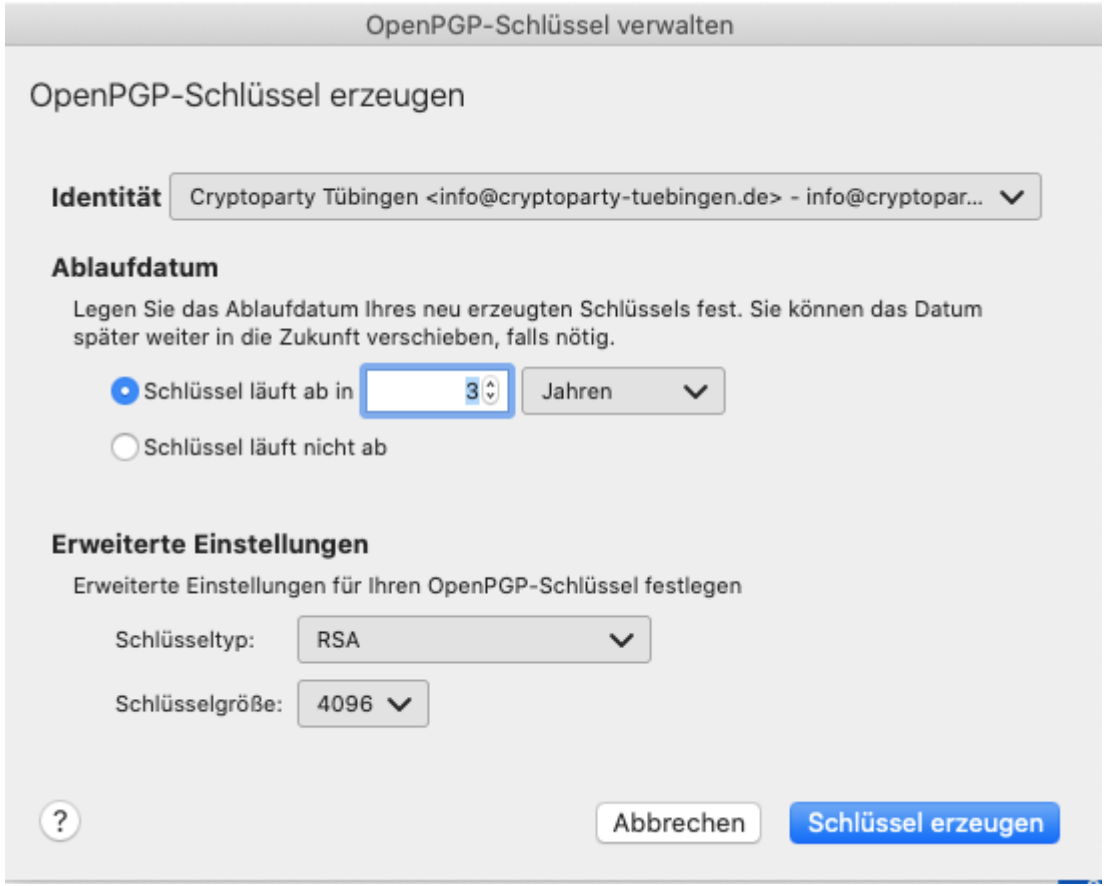
Man sieht zunächst ein leeres Formular, den noch leeren Schlüsselbund.



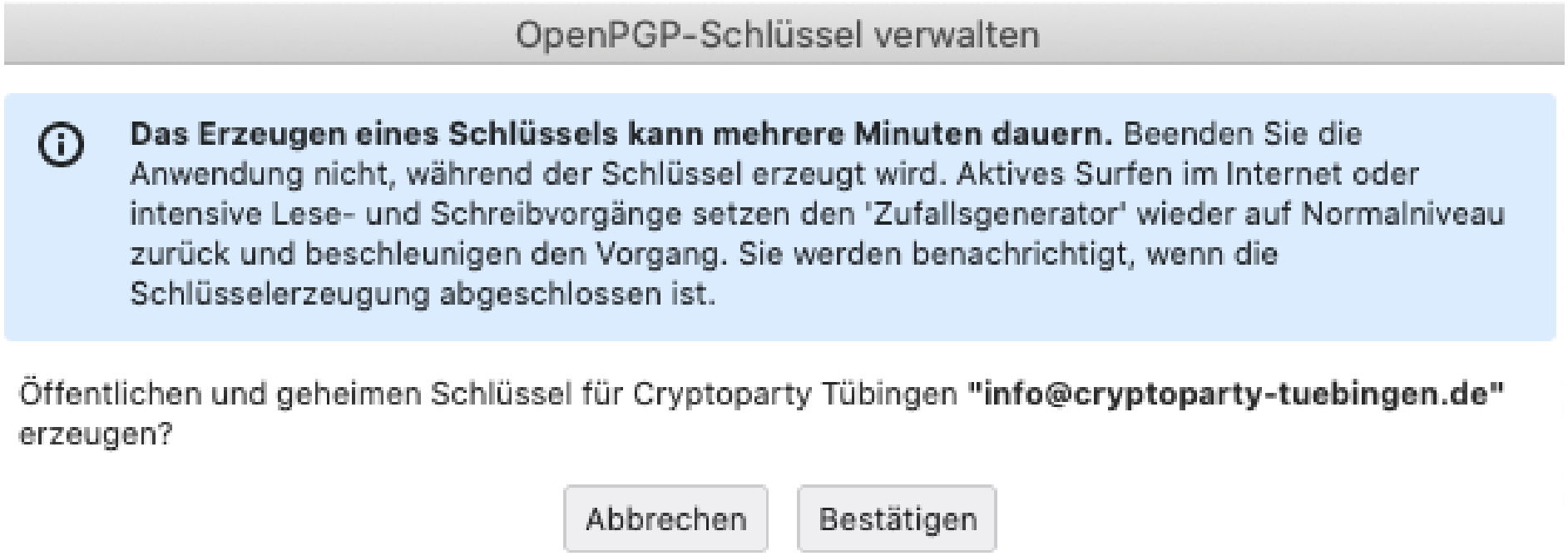
3) Unter „Erzeugen“ kann jetzt das eigene Schlüsselpaar (privater mit öffentlichem Schlüssel) erzeugt werden. „Neues Schlüsselpaar“



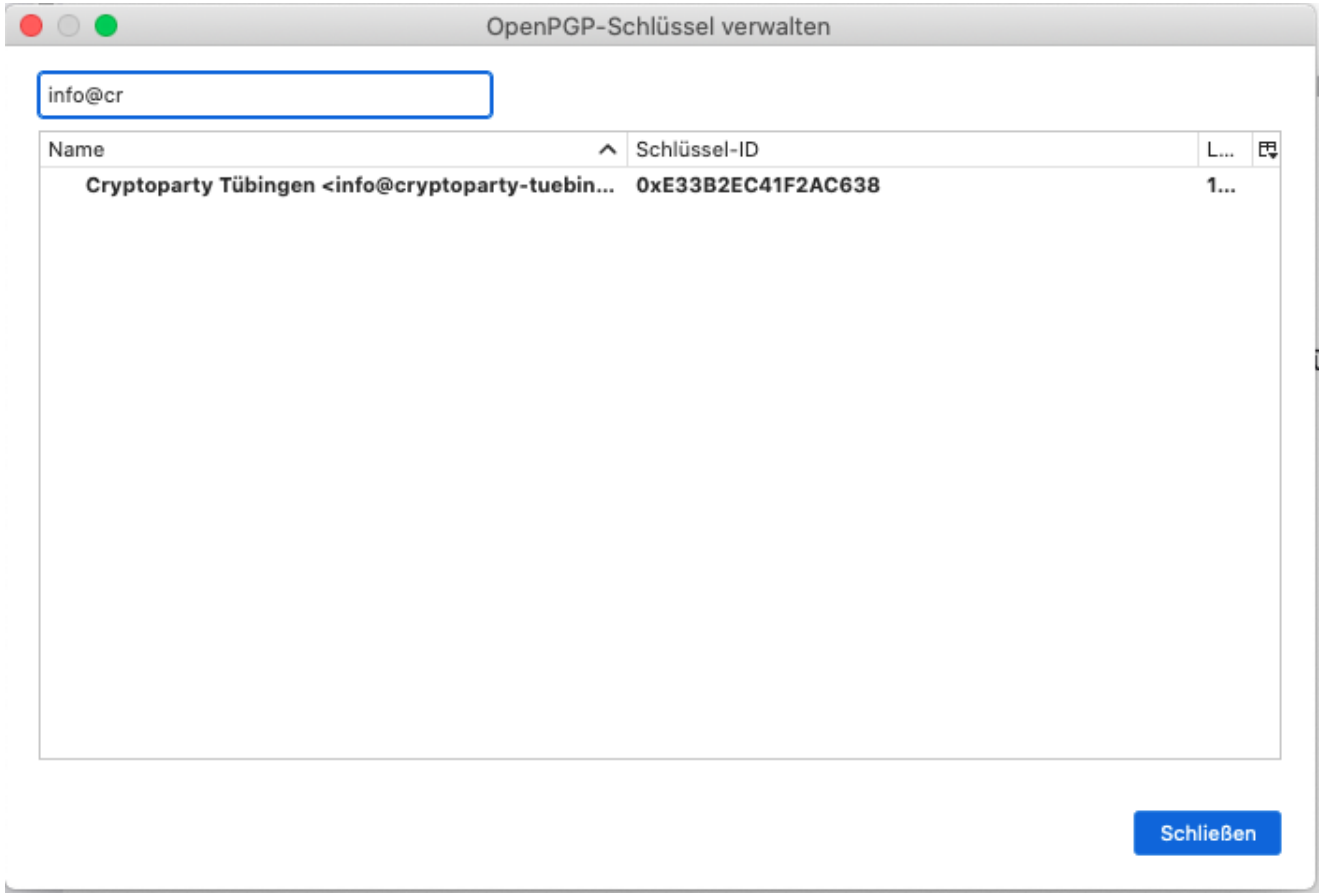
4) Man legt dabei zunächst die Identität fest, d.h. die Zugehörigkeit zur
- E-Mail-Adresse
- Ablaufdatum des Schlüssels (Gültigkeitsdauer)
- Schlüsseltyp: RSA
- Schlüsselgröße: 4096



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



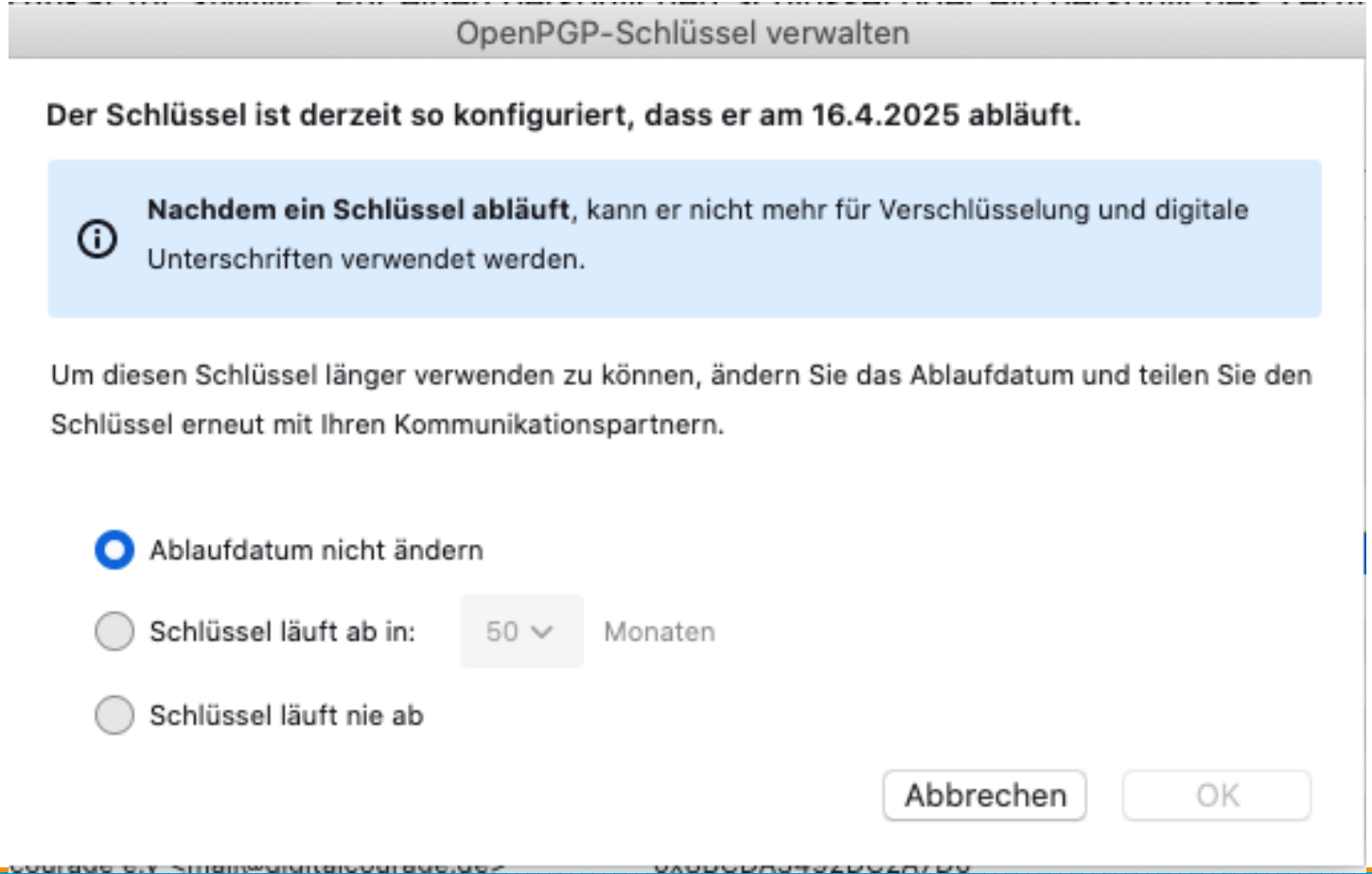
5) Anschließend ist der persönliche PGP-Schlüssel (privat+öffentlich in Fettschrift!) im zuvor leeren Schlüsselbund zu sehen.



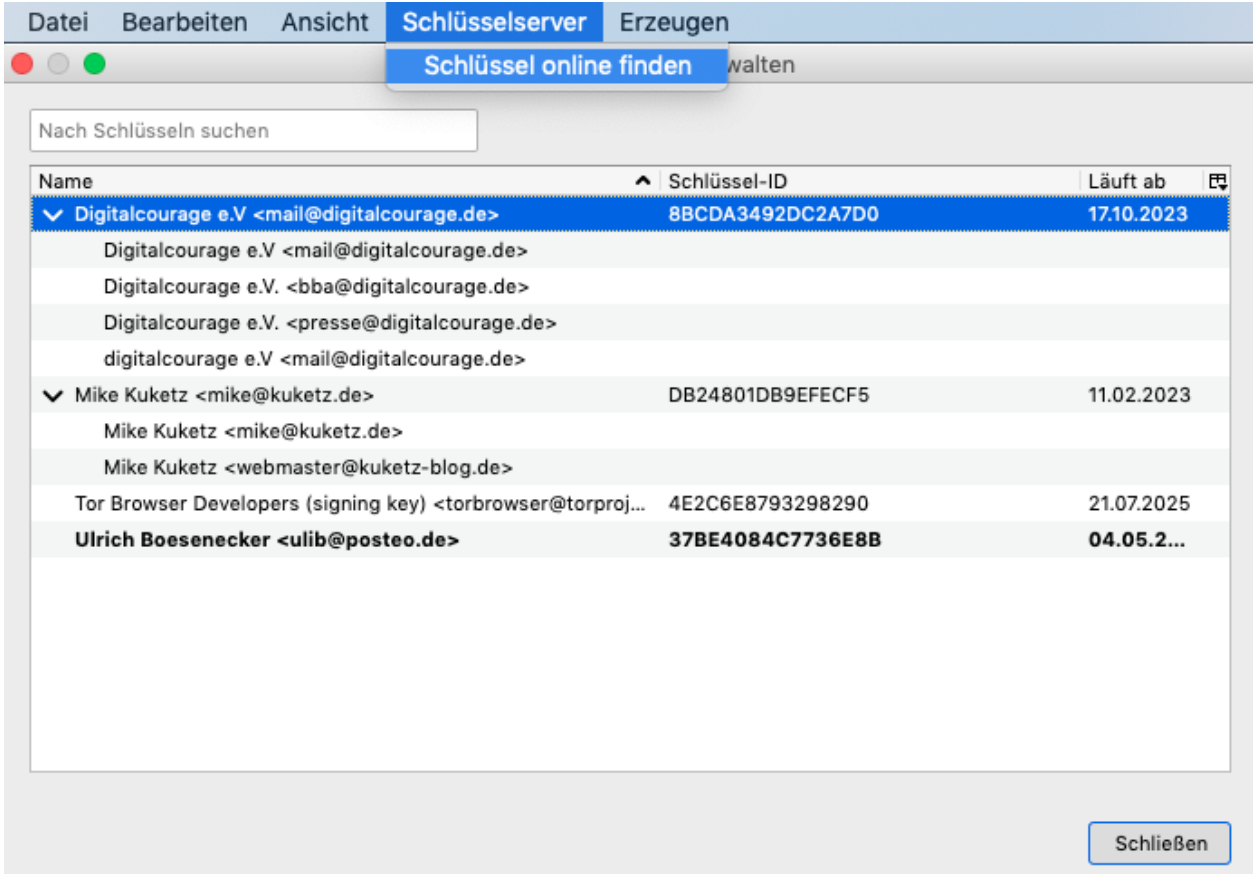
6) Doppelklick auf diesen Eintrag zeigt die Eigenschaften im Einzelnen.

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

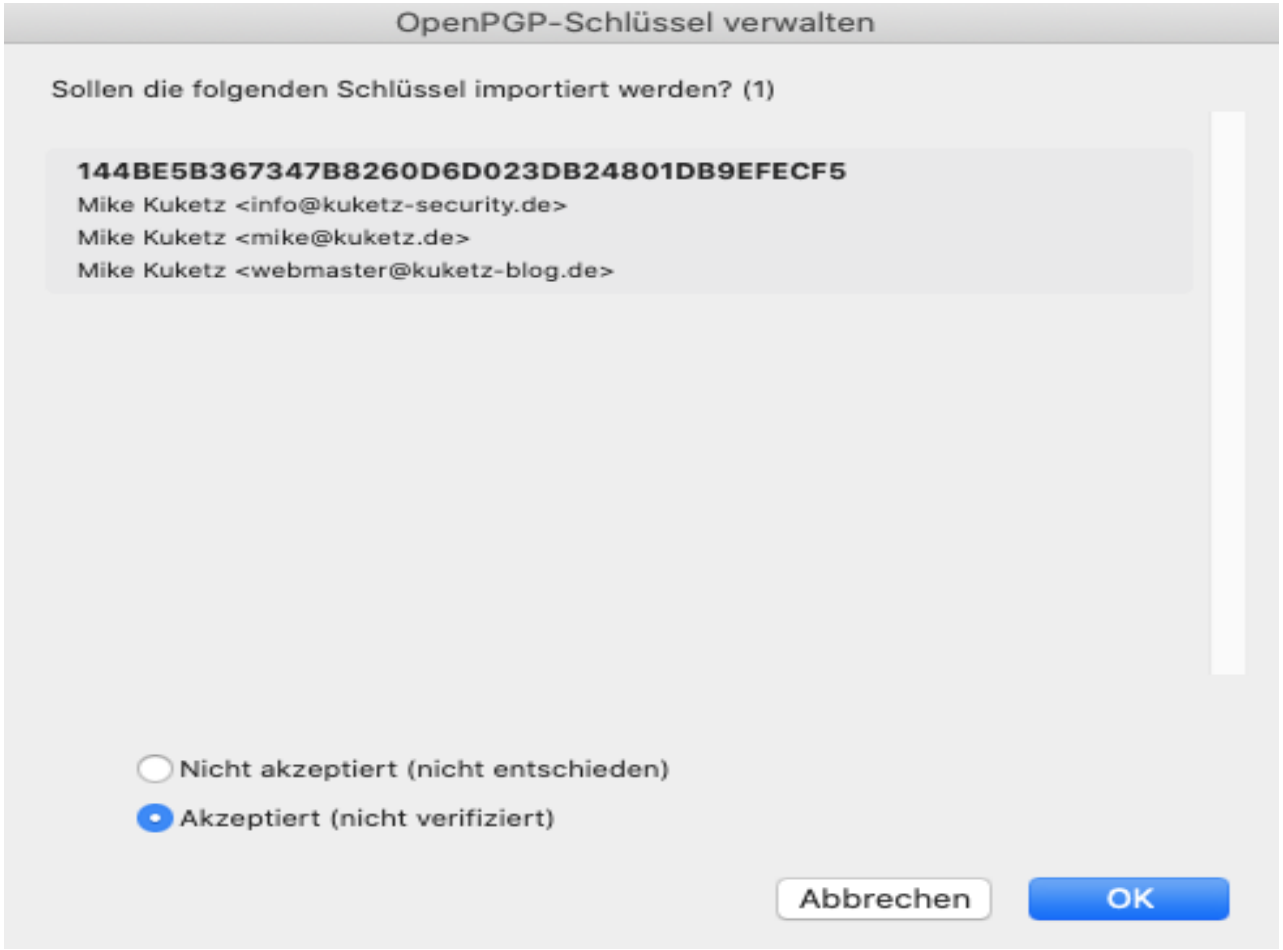
In diesem Formular kann auch später noch das Ablaufdatum geändert bzw. verlängert werden, sogar wenn das Ablaufdatum überschritten ist.



7a) 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.



7b) „Akzeptiert“bestätigen dabei nicht vergessen

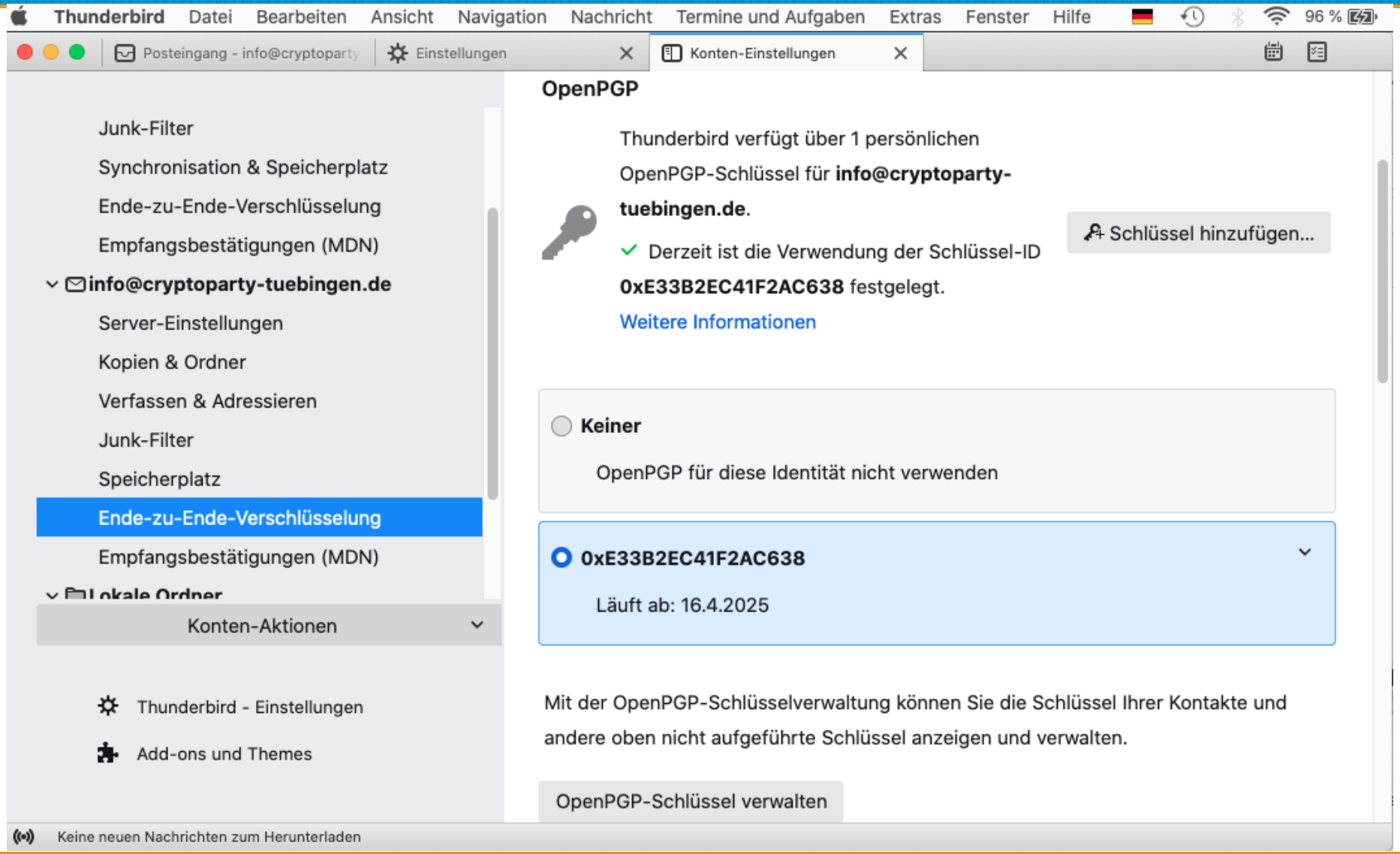


8) Der unterste Menüpunkt unter „Extras“ in Thunderbird ist „Konten-Einstellungen“

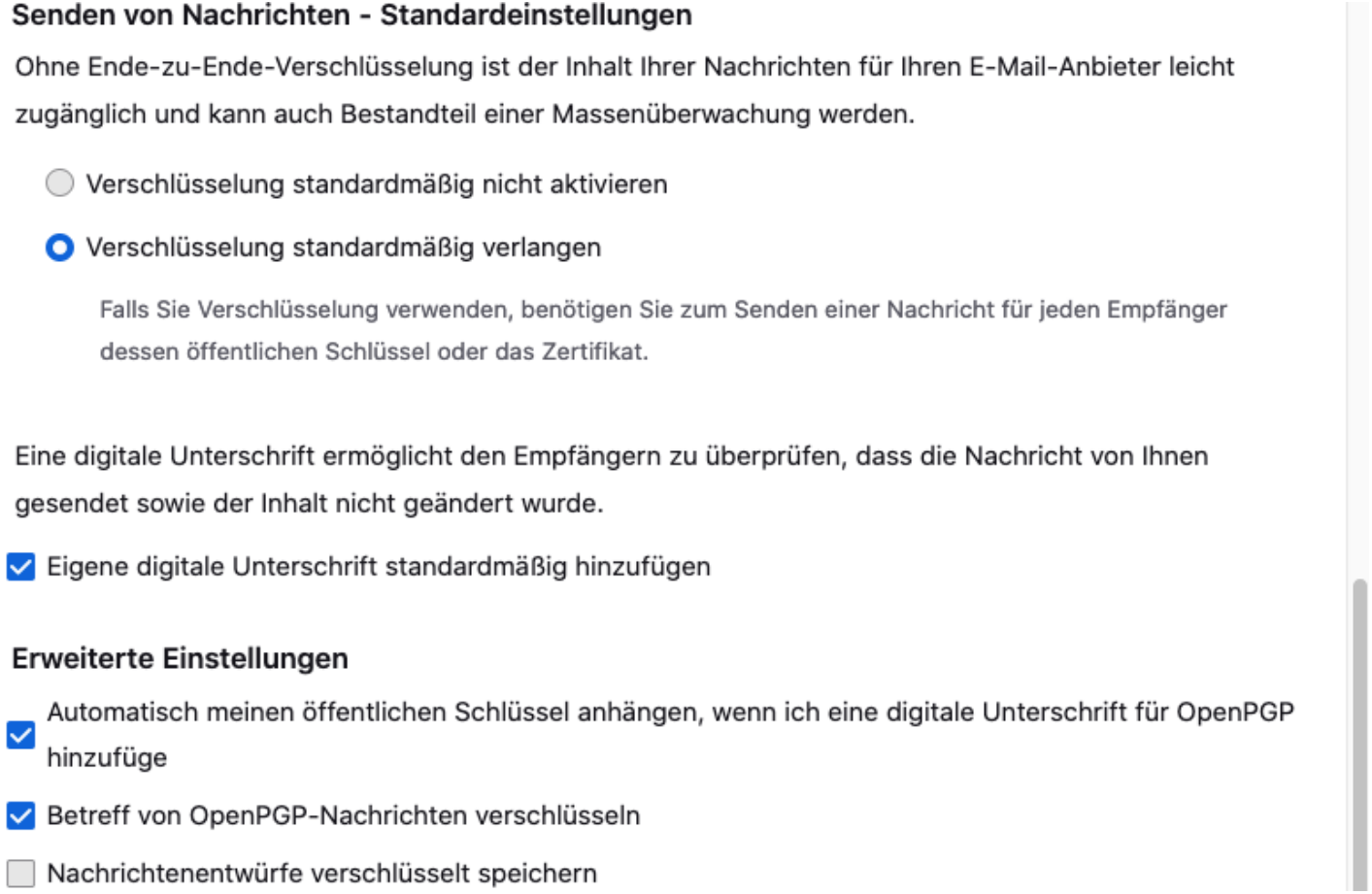
mit dem Unterpunkt „Ende-zu-Ende-Verschlüsselung“

(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.)

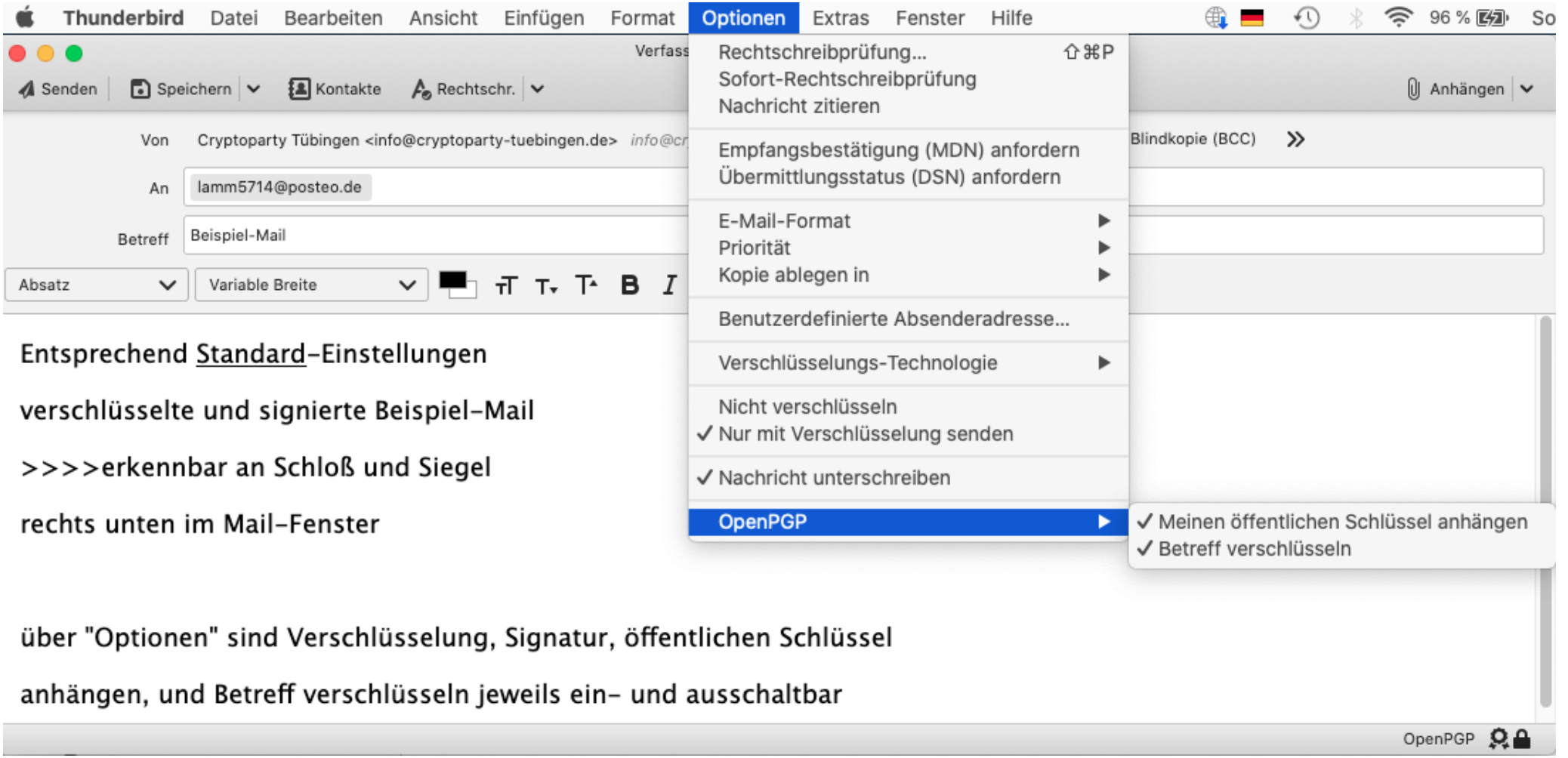
„Keiner“ läßt eine getroffene Vorauswahl im Fall erneuter Erzeugung eines persönlichen Schlüsselpaars nachträglich korrigieren


Thunderbird Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Extras Fenster Hilfe
96 %
Posteingang - info@cryptoparty
Einstellungen
Konten-Einstellungen
Junk-Filter
Synchronisation & Speicherplatz
Ende-zu-Ende-Verschlüsselung
Empfangsbestätigungen (MDN)
info@cryptoparty-tuebingen.de
Server-Einstellungen
Kopien & Ordner
Verfassen & Adressieren
Junk-Filter
Speicherplatz
Ende-zu-Ende-Verschlüsselung
Empfangsbestätigungen (MDN)
Lokale Ordner
Konten-Aktionen
Thunderbird - Einstellungen
Add-ons und Themes
OpenPGP
Thunderbird verfügt über 1 persönlichen OpenPGP-Schlüssel für info@cryptoparty-tuebingen.de.
Derzeit ist die Verwendung der Schlüssel-ID 0xE33B2EC41F2AC638 festgelegt.
Weitere Informationen
Schlüssel hinzufügen...
Keiner
OpenPGP für diese Identität nicht verwenden
0xE33B2EC41F2AC638
Läuft ab: 16.4.2025
Mit der OpenPGP-Schlüsselverwaltung können Sie die Schlüssel Ihrer Kontakte und andere oben nicht aufgeführte Schlüssel anzeigen und verwalten.
OpenPGP-Schlüssel verwalten
Keine neuen Nachrichten zum Herunterladen

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



Verschlüsselung und Signatur ist beim Verfassen an Symbolen erkennbar und einstellbar.



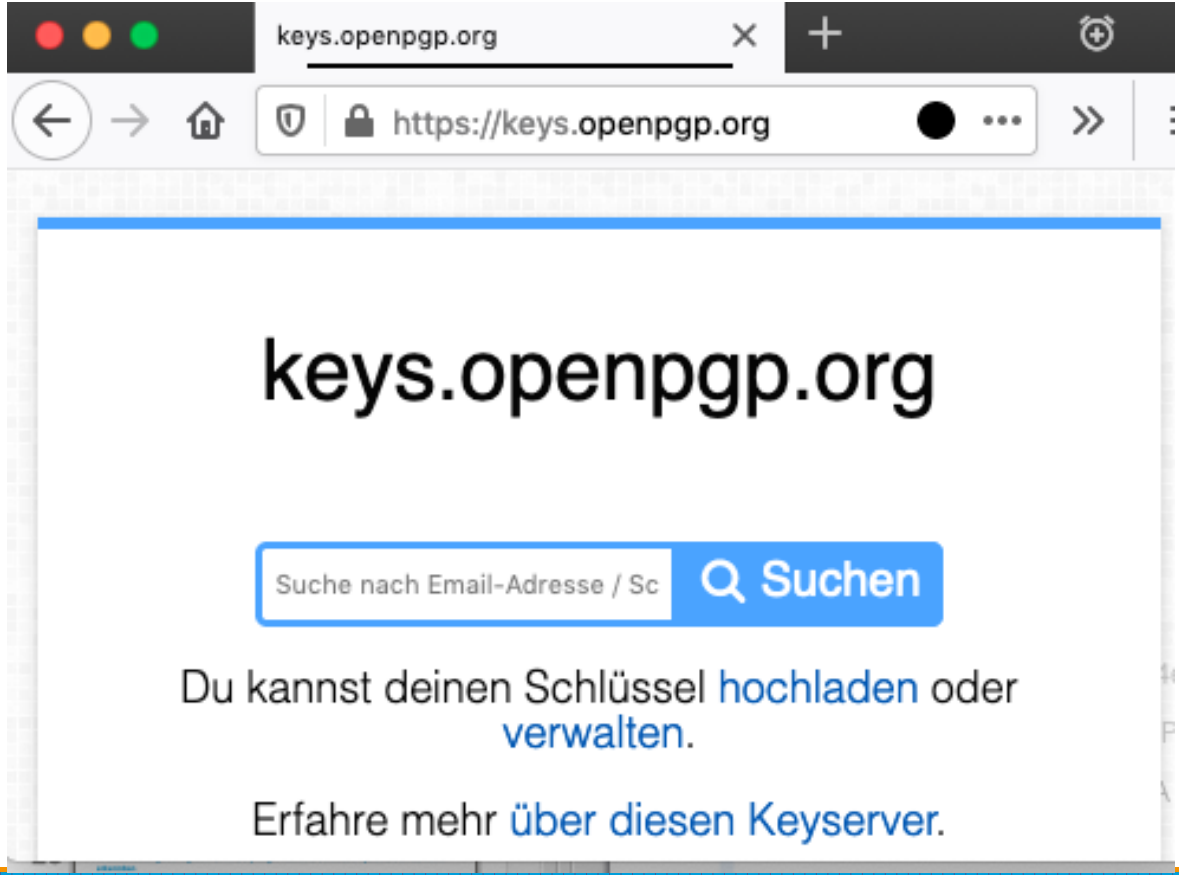
Auch kann der eigene öffentliche Schlüssel für die Rückantwort und für den Schlüsselbund eines PGP-Partner-Empfängers automatisch mitgesendet werden.

Keine Sorge!

„Nichtverschlüssler“

werden ganz normal von unverschlüsselten E-Mails erreicht.

10) Eine weitere Schlüssel-Verteilmethode geht über einen Schlüsselserver: 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?