

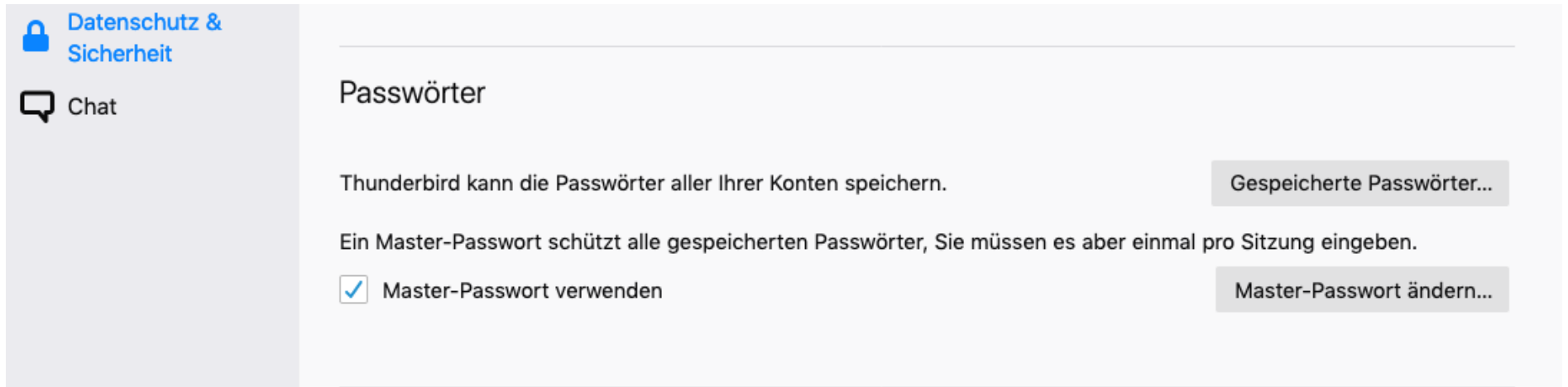
E-Mail-Verschlüsselung im E-Mail-Client Thunderbird ab Version 78 Praktische Durchführung

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

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

Die Optik auf anderen Betriebssystemen kann leicht abweichen.

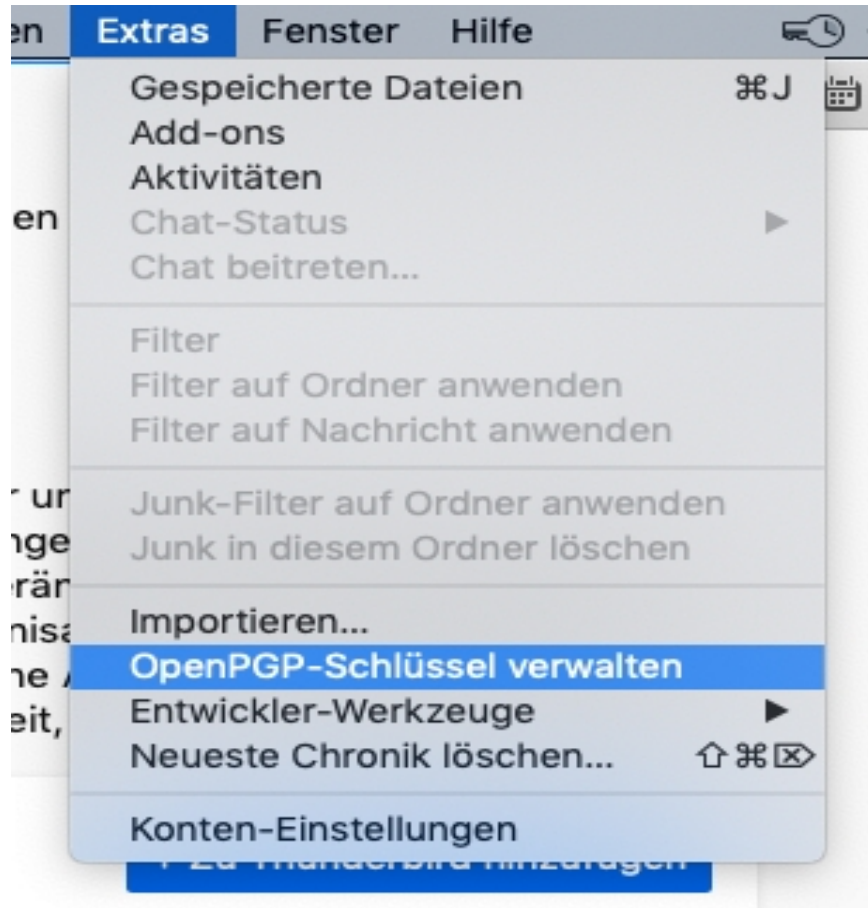
1) In „Einstellungen/ Datenschutz + Sicherheit“ von Thunderbird ein Master-Passwort vergeben und gut merken bzw. sicher verwahren. Dieses dient später dem Schutz und der bedarfsweisen Nutzung des Privaten PGP-Schlüssels, solange das Programm Thunderbird geöffnet ist. Nur dieses Master-Passwort erschließt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



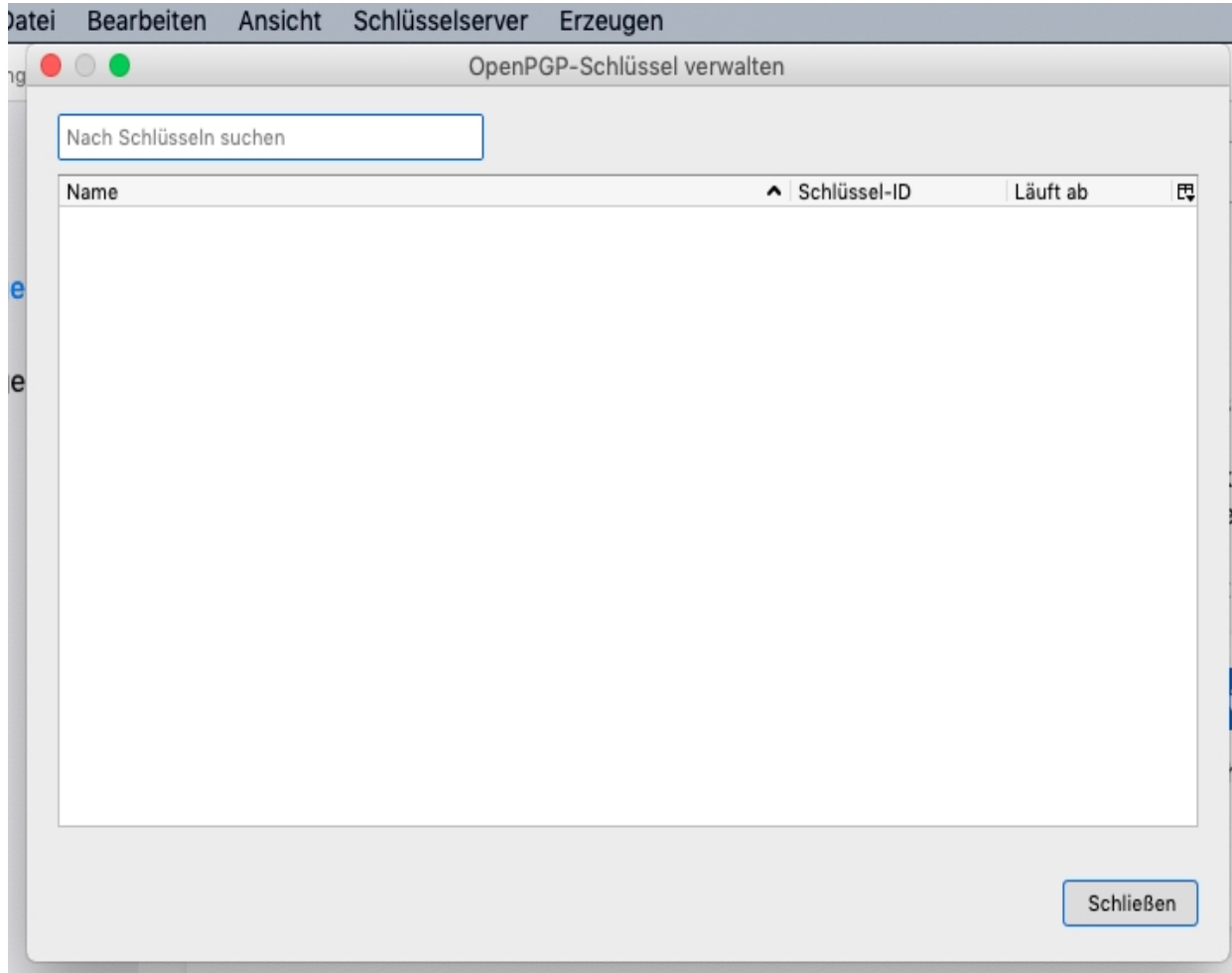
The screenshot shows the 'Datenschutz & Sicherheit' (Data Protection & Security) settings page in Thunderbird. The left sidebar contains a lock icon for 'Datenschutz & Sicherheit' and a speech bubble icon for 'Chat'. The main content area is titled 'Passwörter' (Passwords). It contains the following text and elements:

- A horizontal line at the top of the main content area.
- The heading 'Passwörter'.
- The text: 'Thunderbird kann die Passwörter aller Ihrer Konten speichern.' (Thunderbird can save the passwords of all your accounts.)
- A button labeled 'Gespeicherte Passwörter...' (Saved passwords...).
- The text: '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.)
- A checked checkbox followed by the text 'Master-Passwort verwenden' (Use master password).
- A button labeled 'Master-Passwort ändern...' (Change master password...).
- A horizontal line at the bottom of the main content area.

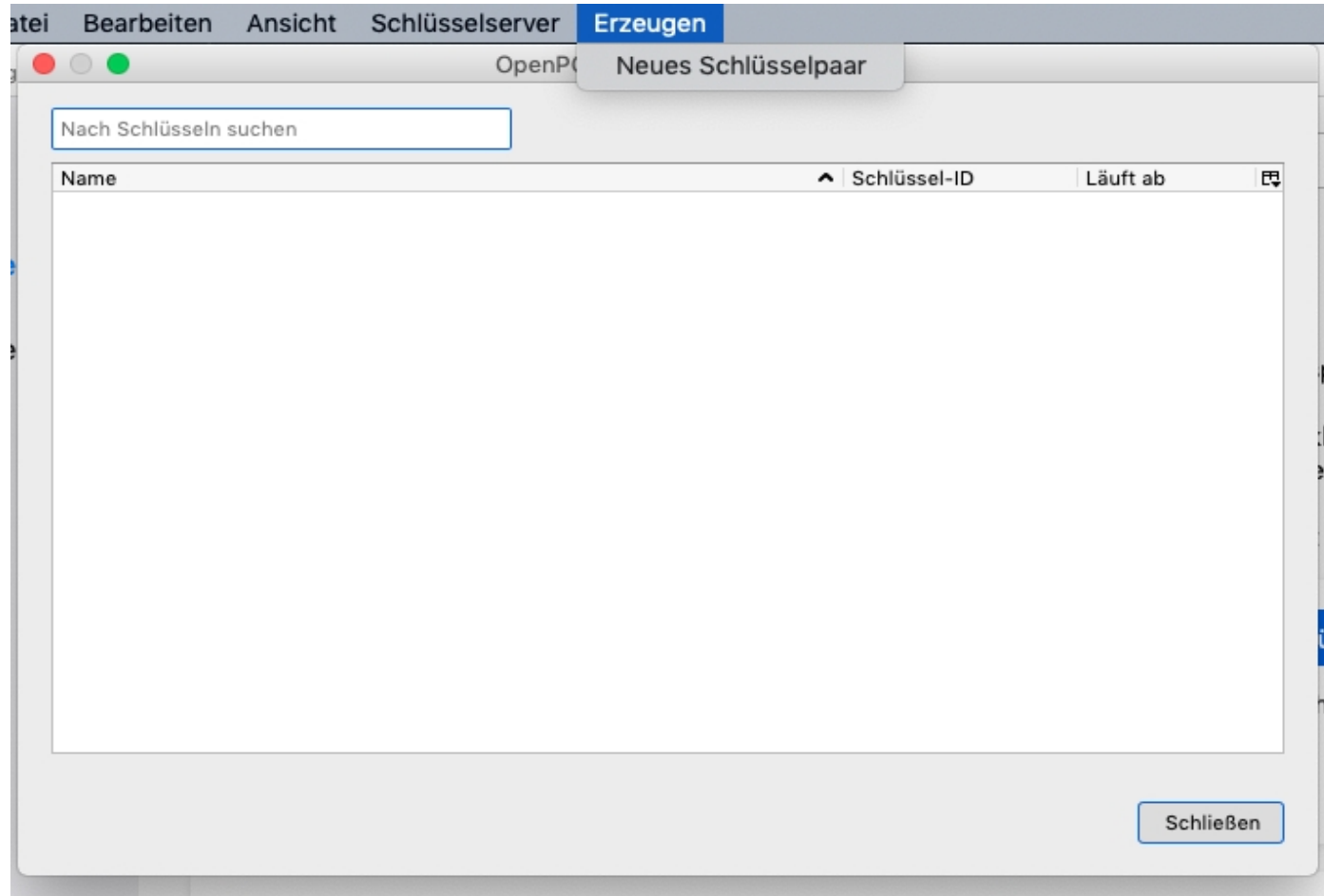
2) Bei geöffnetem Programm Thunderbird unter „Extras“ den Menü-Punkt „Open-PGP-Schlüssel verwalten“ aufrufen



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

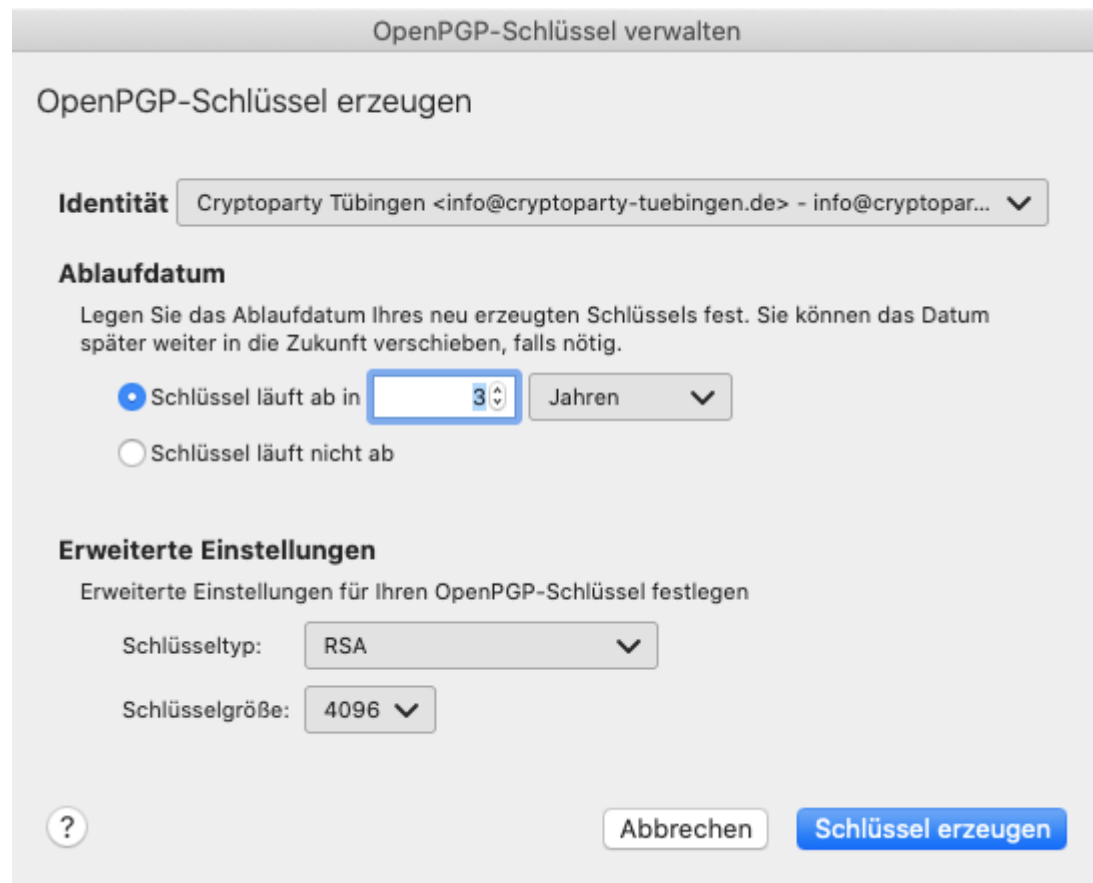


3) Unter „Erzeugen“ kann jetzt das eigene Schlüsselpaar (privater mit öffentlichem Schlüssel) erzeugt werden. „Neues Schlüsselpaar“



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

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



The screenshot shows a web interface titled "OpenPGP-Schlüssel verwalten" with a sub-section "OpenPGP-Schlüssel erzeugen".

Identität

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 Jahren

Schlüssel läuft nicht ab

Erweiterte Einstellungen
Erweiterte Einstellungen für Ihren OpenPGP-Schlüssel festlegen

Schlüsseltyp:

Schlüsselgröße:

Buttons:

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

OpenPGP-Schlüssel verwalten



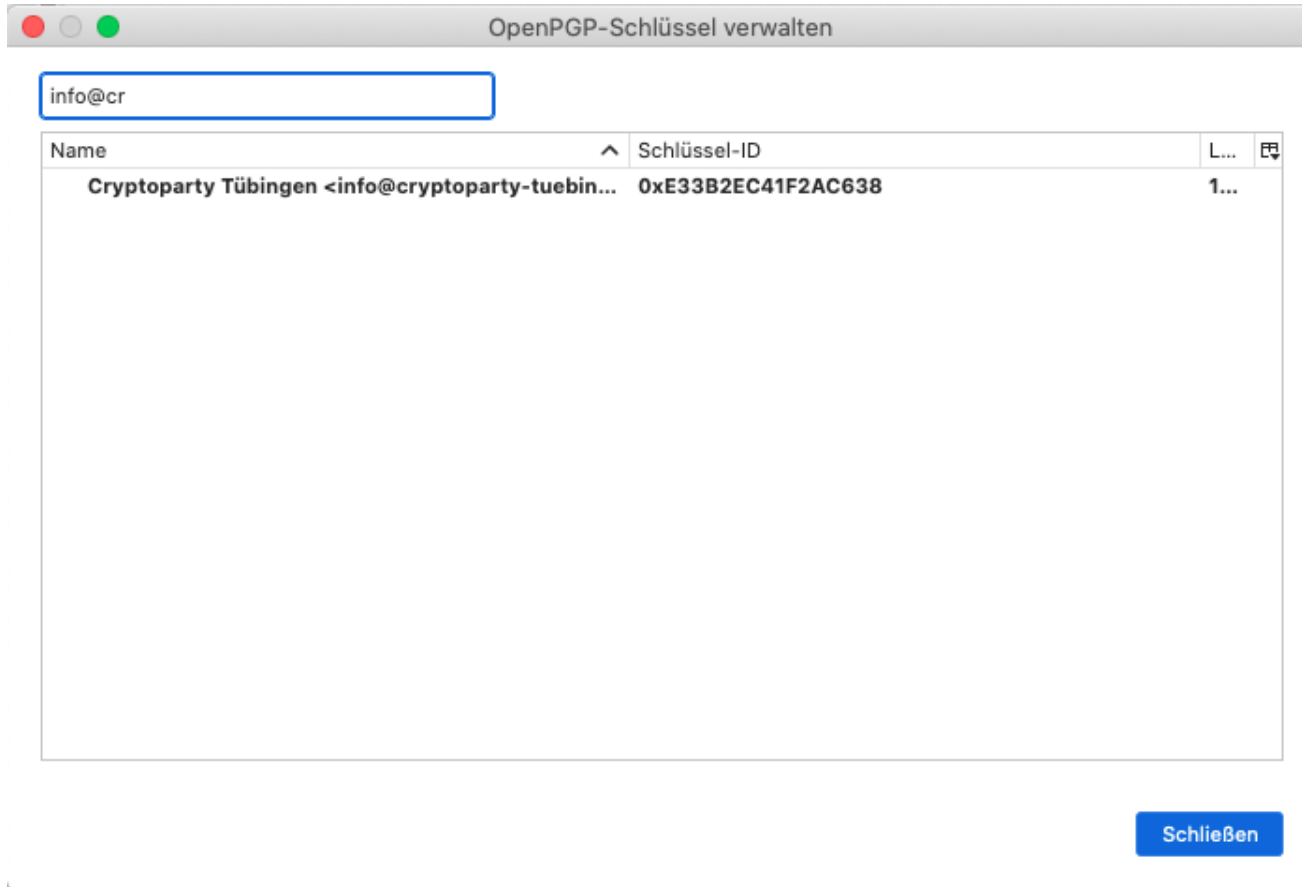
Das Erzeugen eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung nicht, während der Schlüssel erzeugt wird. Aktives Surfen im Internet oder intensive Lese- und Schreibvorgänge setzen den 'Zufallsgenerator' wieder auf Normalniveau zurück und beschleunigen den Vorgang. Sie werden benachrichtigt, wenn die Schlüsselerzeugung abgeschlossen ist.

Öffentlichen und geheimen Schlüssel für Cryptoparty Tübingen "info@cryptoparty-tuebingen.de" erzeugen?

Abbrechen

Bestätigen

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.

OpenPGP-Schlüssel verwalten

Vorgeblicher Schlüsselbesitzer	Cryptoparty Tübingen <info@cryptoparty-tuebingen.de>
Typ	Schlüsselpaar (geheimer Schlüssel und öffentlicher Sch
Fingerabdruck	FD63 C245 F29D 38E3 2807 EB75 E33B 2EC4 1F2A C6
Erzeugt am	17.4.2022
Läuft ab am	16.4.2025

[Ablaufdatum ändern](#)

[Ihre Akzeptanz](#) [Zertifizierungen](#) [Struktur](#)

Sie verfügen sowohl über den öffentlichen als auch über den geheimen Teil dieses Schlüssels und können ihn daher als persönlichen Schlüssel verwenden. Falls Sie diesen Schlüssel von einer anderen Person erhalten haben, dürfen Sie diesen nicht als persönlichen Schlüssel verwenden.

Haben Sie den Schlüssel selbst erzeugt und gibt der Schlüssel Sie als Besitzer aus?

Nein, nicht als meinen persönlichen Schlüssel verwenden.

Ja, als meinen persönlichen Schlüssel verwenden.

[OK](#)

> 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.

OpenPGP-Schlüssel verwalten

Der Schlüssel ist derzeit so konfiguriert, dass er am 16.4.2025 abläuft.

i **Nachdem ein Schlüssel abläuft**, kann er nicht mehr für Verschlüsselung und digitale Unterschriften verwendet werden.

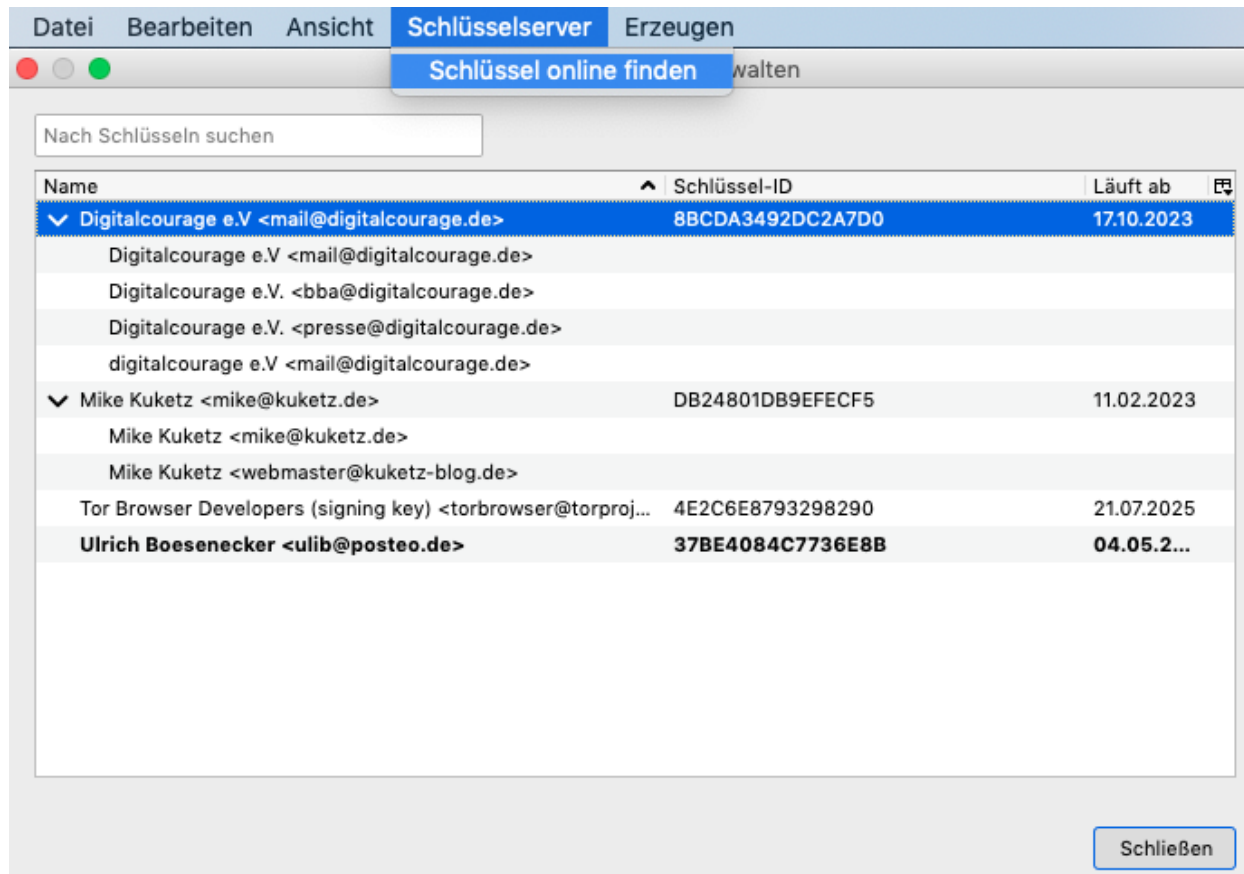
Um diesen Schlüssel länger verwenden zu können, ändern Sie das Ablaufdatum und teilen Sie den Schlüssel erneut mit Ihren Kommunikationspartnern.

Ablaufdatum nicht ändern

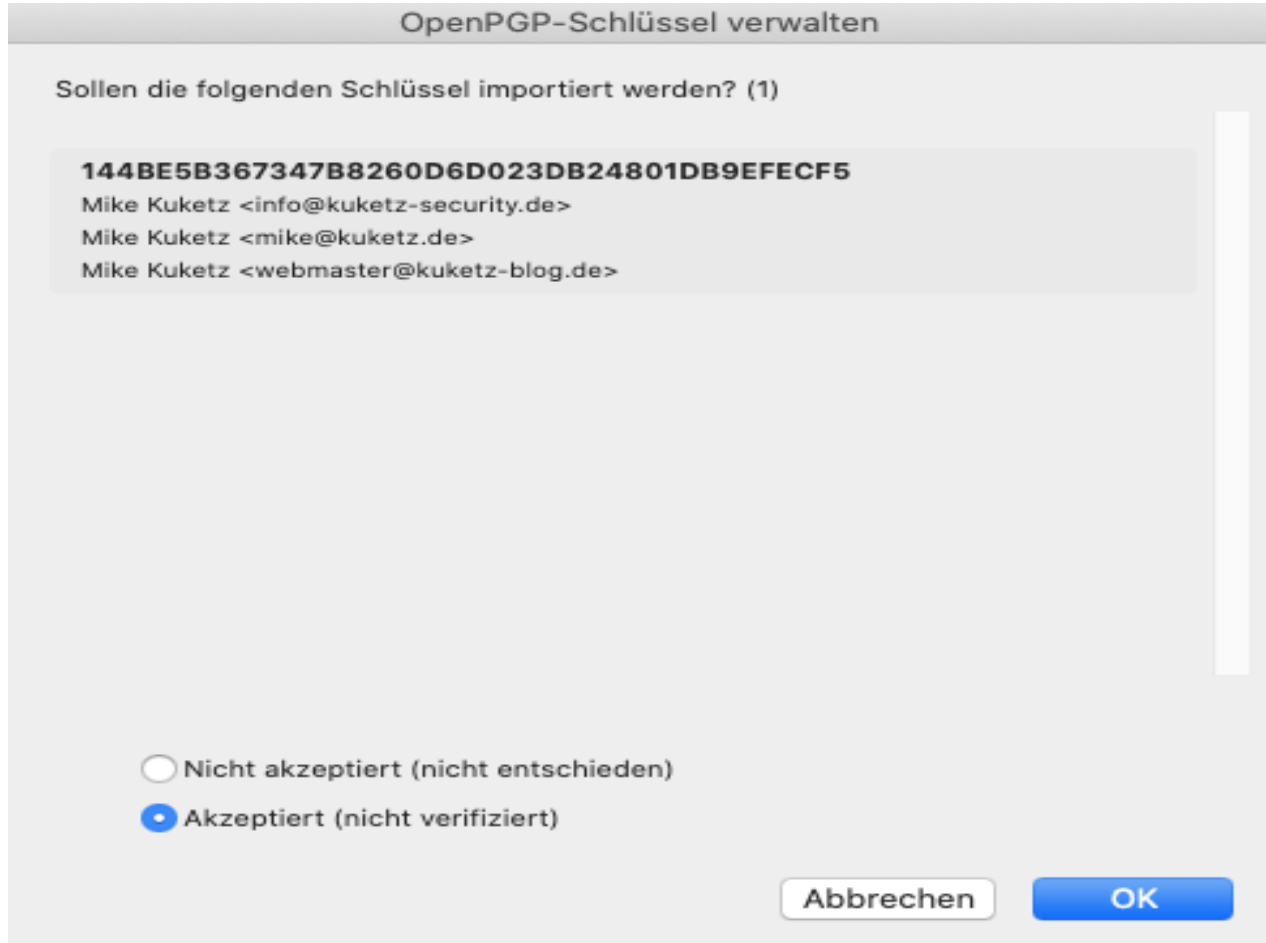
Schlüssel läuft ab in:

Schlüssel läuft nie ab

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

- 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

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.

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.

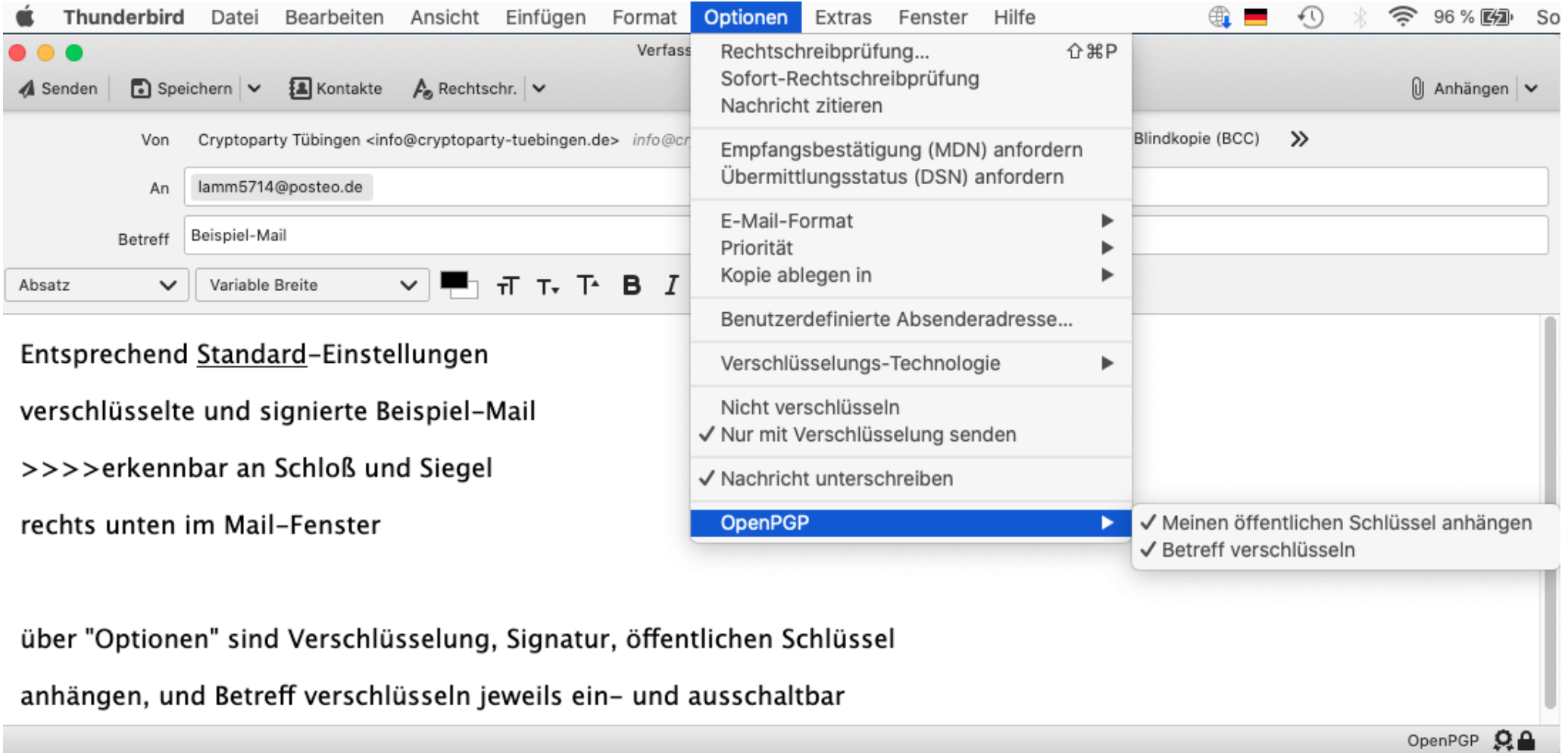
Eine digitale Unterschrift ermöglicht den Empfängern zu überprüfen, dass die Nachricht von Ihnen gesendet sowie der Inhalt nicht geändert wurde.

- Eigene digitale Unterschrift standardmäßig hinzufügen

Erweiterte Einstellungen

- Automatisch meinen öffentlichen Schlüssel anhängen, wenn ich eine digitale Unterschrift für OpenPGP hinzufüge
- Betreff von OpenPGP-Nachrichten verschlüsseln
- Nachrichtenentwürfe verschlüsselt speichern

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



The screenshot shows the Thunderbird 'Options' menu for a new email. The 'OpenPGP' option is selected, and its sub-menu is visible, showing the following options:

- Meinen öffentlichen Schlüssel anhängen
- Betreff verschlüsseln

The main menu also shows other options like 'Rechtschreibprüfung...', 'Sofort-Rechtschreibprüfung', 'Nachricht zitieren', 'Empfangsbestätigung (MDN) anfordern', 'Übermittlungsstatus (DSN) anfordern', 'E-Mail-Format', 'Priorität', 'Kopie ablegen in', 'Benutzerdefinierte Absenderadresse...', and 'Verschlüsselungs-Technologie'.

Entsprechend Standard-Einstellungen

verschlüsselte und signierte Beispiel-Mail

>>>>erkennbar an Schloß und Siegel

rechts unten im Mail-Fenster

über "Optionen" sind Verschlüsselung, Signatur, öffentlichen Schlüssel

anhängen, und Betreff verschlüsseln jeweils ein- und ausschaltbar

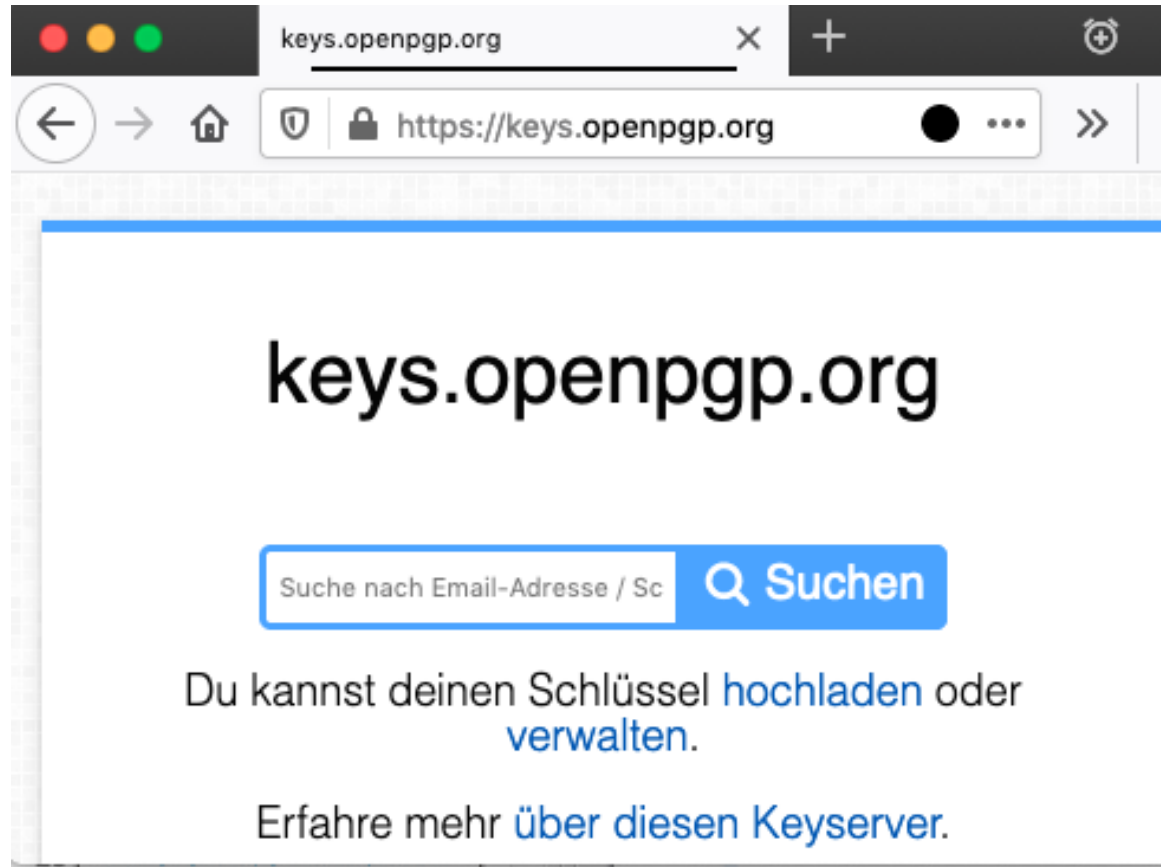
Auch kann der eigene öffentliche Schlüssel für die Rückantwort und für den Schlüsselbund eines PGP-Partner-Empfängers automatisch mitgesendet werden.

Keine Sorge!

„Nichtverschlüssler“

werden ganz normal von unverschlüsselten E-Mails erreicht.

10) Eine weitere Schlüssel-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?