HowTo: Veschlüsselung mit Thunderbird 78

EG HH - Technik AG

14. Dezember 2020 Version 1.0.3

PDF-Download • Online-Version Web: https://www.ende-gelaende-hamburg.info/technik/ Code: https://codeberg.org/EG-HH/HowTo-Thunderbird78-PGP/

Inhaltsverzeichnis

1	Einführung	2
2	Für Enigmail-Umsteiger*innen	4
3	Eigene PGP-Schlüssel verwalten 3.1 PGP-Schlüssel erzeugen 3.2 Einstellungen ändern	7 8 9
4	Master-Passwort anlegen	10
5	Einen öffentlichen Schlüssel importieren	12
6	Schlüssel überprüfen & akzeptieren 6.1 Neue Schlüssel beim Importieren akzeptieren 6.2 Gespeicherte PGP-Schlüssel akzeptieren	13 13 14
7	Eine verschlüsselte E-Mail schreiben	16
8	Eine Nachricht entschlüsseln	17

DOMAIN

Diese Anleitung ist gemeinfrei nach Creative Commons CC0. Davon ausgenommen sind die Teile der Bildschirmfoto, die Mozilla Thunderbird und Enigmail zeigen, welche unter der Mozilla Public License, Version 2.0 lizensiert sind. Mozilla, Thunderbird und das Thunderbird Logo sind Marken der Mozilla Foundation.

1 Einführung

Das E-Mail-Programm Thunderbird hat vor kurzem ein großes Update bekommen, das einiges daran verändert, wie Thunderbird mit verschlüsselten E-Mails umgeht. Bisher musste man das Addon *Enigmail* installieren, um E-Mails zu ver- und entschlüsseln. Mit der neuen Thunderbird-Version ist das nun nicht mehr nötig - Thunderbird unterstützt von sich aus verschlüsselte E-Mails. Du musst aber einmalig ein paar Einstellungen verändern und dich ein bisschen umgewöhnen. In dieser Anleitung zeigen wir dir, wie du den Umstieg schaffst und E-Mails mit Thunderbird verschlüsseln kannst. Viele weitere Fragen, die bei der Nutzung von E-Mail-Verschlüsselung in Thunderbird auftreten könnten, werden hier beantwortet: https://support.mozilla.org/de/kb/openpgp-thunderbird-howto-and-faq

Wenn du noch wenig oder keine Erfahrung mit E-Mail-Verschlüsselung hast, sieh dir dieses Video an, das das Prinzip einfach erklärt: https://youtube.com/watch?v=4mbryW8fZrA

Folgende Prinzipien solltest du verinnerlichen:

- Verschlüsselung verhindert das unberechtigte Lesen einer Nachricht.
- Eine digitale Unterschrift verhindert¹ das unberechtigte Verändern einer Nachricht.
- Um eine Nachricht zu verschlüsseln, benötigst du den öffentlichen Schlüssel der Empfänger*in.
- Um eine Nachricht zu entschlüsseln, benötigst du deinen geheimen Schlüssel.
- Um eine Nachricht zu unterschreiben, benötigst du deinen geheimen Schlüssel.
- Um eine Unterschrift zu prüfen, benötigst du den öffentlichen Schlüssel der Absender*in.

¹Um ganz genau zu sein: Auch digital unterschriebene Nachrichten können manipuliert werden. Die Empfänger*in kann diese Manipulation jedoch aufdecken, weil die Unterschrift nicht mehr stimmt.

Abbildung 1: Überprüfe zuerst, welche Thunderbird-Version bei dir installiert ist:

(a) Klicke im Menü auf "Hilfe"

(b) ... und dann auf "Über Thunderbird".



(c) Hier ist Version 68.12.0 installiert.



(d) So sieht es nach dem Update aus: Thunderbird Version 78.4.0



Wenn bei dir Thunderbird 68 installiert ist, dann hast du noch die alte Version und die funktioniert wie gewohnt mit Enigmail. Wie du Thunderbird aktualisierst, erfährst du hier: https://support.mozilla.org/de/kb/thunderbird-aktualisieren

Wenn bei dir Thunderbird 78 installiert ist, dann hast du das Update schon erhalten. Wenn du bisher Enigmail benutzt, ließ bitte das nächste Kapitel.

2 Für Enigmail-Umsteiger*innen

Wenn du zum ersten Mal E-Mails verschlüsseln möchtest, kannst du diesen Abschnitt überspringen.

Nach dem Update auf Version 78 sollte dir automatisch dieses Fenster angezeigt werden, das dich darüber infomiert, dass du Enigmail nicht mehr benötigst, und dich aufgefordert, deine PGP-Schlüssel zu übertragen. Sollte das Fenster nicht auftauchen oder hast du es bereits geschlossen, dann kannst du es im Menü öffnen.

Abbildung 2: Thunderbird informiert dich darüber, dass du Enigmail nicht mehr benötigst.

Klicke auf "Migration jetzt starten"



Abbildung 3: Das Fenster zur Übertragung der PGP-Schlüssel kannst du dir erneut anzeigen lassen:

(a) Klicke im Menü auf "Extras"

(b) ... und dann auf "Enigmail-Einstellungen migrieren".

♀ Abrufen ◇ ♪ Verfassen ▲ Adressbuch ◇ Schlagwörter ◇ ♥ Schnellfilter ◇ ♀ crypto-alosteo.net ☆ ♀ Ungelesen ☆ Gekennzeichnet ≧ Kontakt ◇ Schlagwörter ◎ Anhang > Diese Nachrif ● Posteingang (2) ▶ ♠ ⊕ Betreff ∞ Betreff ∞ Betreff ∞ Betreff		Abrufen	Schnellfilter	=
✓ @ crypto-alosteo.net ☆ □ Ungelesen ☆ Gekennzeichnet ▲ Kontakt Schlagwörter □ Anhang > Diese Nachr ✓ Posteingang (2) → 0 Betreff ∞ Betreff ∞ Betreff 0 Anhang	>	v Compto al octao not		· · · · · · · · · · · · · · · · · · ·
 Entwirte Welcome to Posteo Posteo Support Posteo Support Posteo Support Suchen Speichern als Postausgang 	Image:	C if yordanizatione A ↓ Ungelesen Greentzeic C isonadet Papierkorb > Betreff C isonadet Papierkorb > Posteingang (2) C isonadet Papierkorb > Posteingang (2) C isonadet Papierkorb > Posteingang (2) C isonadet Papierkorb > > C isonadet Postausgang > >	hnet Anhang Polese Nacl * Betelligte • Posteo Support • Posteo Support	hri C Extras Adressbuch Strg+Umschalt+8 Filter auf Ordner anwenden Filter auf Ordner anwenden Junk in diesem Ordner löschen Gespeicherte Dateien Strg+J Importieren OgenPG-Schlüssel verwalten Entwickler-Werkzeuge > Neueste Chro Strg+Umschalt+Entf Atkivitäten Enigmail-Einstellungen migrieren
∲•) Un	gelesen: 2 Gesamt: 2	(m)		Ungelesen: 2 Gesamt: 2

Abbildung 4: Der Assistent ist übersichtlich. Du wirst mehrfach aufgefordert, die Passwörter für deine PGP-Schlüssel einzugeben.

(a) Klicke auf "Migration starten"	${\rm (b)} \ {\bf Gib} \ {\bf deine} \ {\bf PGP-Passwörter} \ {\bf ein} \ {\bf und} \ {\bf klicke} \ {\bf am} \ {\bf Ende} \ {\bf auf} \ {\bf ,Fe}$
	🌎 Übertragen Sie Ihre Enigmail-Einstellungen zu Th 🔺 🗵 🔇
Dieser Assistent wird Ihre Schlüssel und Einstellungen aus Enigmail und GnuPG exportieren und importiert sie in den Thunderbird-Schlüsselspeicher.	Dieser Assistent wird Ihre Schlüssel und Einstellungen aus Enigmail und GnuPG exportieren und importiert sie in den Thunderbird-Schlüsselspeicher.
Bitte klicken Sie auf die Schaltfläche 'Migration starten', um mit der Migration zu beginnen	Bitte klicken Sie auf die Schaltfläche 'Migration starten', um mit der Migration zu beginnen.
Der Migration 2d Beginnen. Der Migrationsprozess exportiert Ihre privaten Schlüssel aus GnuPG und importiert sie in Thunderbird. Wenn Ihre Schlüssel durch ein Passphrase geschützt sind, werden Sie aufgefordert, dieses für jeden Schlüssel einzugeben - einmal beim Export aus GnuPG und einmal für den Import in Thunderbird	Der Migrationsprozess exportiert Ihre privaten Schlüssel aus GnuPG und importiert sie in Thunderbird. Wenn Ihre Schlüssel durch ein Passphrase geschützt sind, werden Sie aufgefordert, dieses für jeden Schlüssel einzugeben - einmal beim Export aus GnuPG und einmal für den Import in Thunderbird.
Migration starten	Migration starten
	Exportiere Schlüssel aus GnuPG 🗸
	Importiere Schlüssel in Thunderbird 🗸
	Übernehme Ihre Kontoeinstellungen 🗸
	Alles erledigt! Enigmail wird nun nicht mehr benötigt und kann deinstalliert werden.
Abbrechen <u>E</u> ertig	Abbrechen <u>F</u> ertig

Die PGP-Schlüssel sind jetzt übernommen worden und können benutzt werden. Falls du eine Fehlermeldung angezeigt bekommst, starte die Migration erneut, das hilft manchmal. Ließ dir bitte auch die folgenden Abschnitte aufmerksam durch, da du noch einige Einstellungen anpassen solltest und sich einige Abläufe minimal verändert haben.

3 Eigene PGP-Schlüssel verwalten

Egal, ob du gerade deine PGP-Schlüssel aus Enigmail importiert hast oder aber noch gar keine PGP-Schlüssel besitzt, öffne in beiden Fällen deine Konto-Einstellungen:

Abbildung 5: Öffne die Konto-Einstellungen:

(a) Klicke im Menü auf "Konten-Einstellungen"

(b) ... und dann auf "Ende-zu-Ende-Verschlüsselung".

Wenn du bereits einen PGP-Schlüssel hast, dann wähle diesen hier aus. Wenn du noch keinen PGP-Schlüssel hast, klicke auf "Schlüssel hinzufügen".

3	Posteingang - Mozilla Thunderbird		≜ - ≎ 🔇	9	Konten-Einstellungen - Mozilla Thunderbird 🗠 – 🕫 🔞
🖵 Abrufen 👻 🖋 Verfassen	🖪 Adressbuch 🛛 🛇 Schlagwörter 🗸 🛛 🖓 Schnellfilter		東	Posteingang Konten-Einstellungen	× 8
 ✓ Crypto-alosteo.net Posteingang (2) Entwürfe ⊲ Gesendet ⊕ Papierkorb ✓ Local Polders ഈ Papierkorb ⊗ Postausgang 	☆ □ Ungelesen ☆Gekennzeichnet ⊡Kontakt \Schlagwörter 1 ◆ ● Betreff ● ● ☆ Welcome to Posteo ● ● ● ● ☆ Posteo payment instructions ● ● ● ● ☆ Posteo payment instructions ● ● ● ● ●	Anhang Poliese Nachri Posteo Support Posteo Support	Neu > Anhänge > Bearbelten ★ ● ● > Drucken > > > Drucken > > > Anhänge > > > Drucken > > > Madons > > Madons > > Mathagen > > > Addons > > Mathagen > > > Anasischt > > > Ansightion > > Nachricht > > Extras > > > Ø Hilfe > > Ø Beenden > >	 C prysto-alice@posteo.net Server-Einstellungen Kopien & Ordner Verfassen & Adressieren Junk-Filter Speicherplatz Orstausgangs-Server (SMTP) 	Ende-zu-Ende-Verschlüsselung Um Nachrichten zu verschlüsseln oder digital zu unterschreiben, muss eine der Verschlüsselungstechnologien OpenPCP oder S/MIME eingerichtet werden. Wählen Sie Ihren persönlichen Schlüssel für die Verwendung von OpenPCP oder Ihr persönliches Zertifikat für S/MIME. Für einen persönlichen Schlüssel oder ein persönliches Zertifikat verfügen Sie über den entsprechenden geheimen Schlüssel. Weitere Informationen OpenPCP Thunderbird verfügt über 1 persönlichen OpenPCP-Schlüssel für cyto-aliec@posteo.net. V * Orzelice@posteo.net. * Orze
(w)			Ungelesen: 2 Gesamt: 2	(iz)	

3.1 PGP-Schlüssel erzeugen

Enigmail-Umsteiger*innen können diesen Schritt überspringen.

Wenn du noch keinen PGP-Schlussel besitzt, solltest du jetzt einen erzeugen.

Abbildung 6: Einen PGP-Schlüssel zu erzeugen geht ganz schnell:

(a) Wähle "Neuen OpenPGP-Schlüssel erzeugen" aus und klicke auf "Weiter"

(b) Hier kannst du die Schlüsselgröße auf 4096 stellen und "Schlüssel erzeugen" anklicken. Im nächsten Fenster musst du noch ein Mal "Bestätigen".



3.2 Einstellungen ändern

Jetzt solltest du im unteren Bereich noch ein paar Einstellungen anpassen. Empfehlenswert sind diese Einstellungen:

- "Verschlüsselung standardmäßig verlangen" Thunderbird wird automatisch versuchen, jede E-Mail, die du schreibst, zu verschlüsseln.
- "Eigene digitale Unterschrift standardmäßig hinzufügen", damit andere überprüfen können, dass eine Nachricht wirklich von dir stammt.



Abbildung 7: Diese Einstellungen solltest du auswählen.

4 Master-Passwort anlegen

Wenn du schon ein Master-Passwort hast, kannst du diesen Abschnitt überspringen.

Deine PGP-Schlüssel sind in Thunderbird 78 nicht mehr durch ein Passwort geschützt! Jede Person, die Zugriff auf deinen Computer hat, kann also deine E-Mails entschlüsseln, ohne ein Passwort eingeben zu müssen. Das kannst du ändern, indem du ein Master-Passwort anlegst. Dieses Passwort sichert auch die Login-Daten für deine E-Mail-Postfächer. Es schützt allerdings nicht unverschlüsselte E-Mails, diese kann man auch ohne Passwort weiterhin lesen.

Posteingang - Mozilla Thunderbird ± - 0 😣 ٢ Einstellungen - Mozilla Thunderbird ± - ∞ 😣 Posteingang 🔆 Einstellungen ÷ 1 × ė 🖻 🕞 Posteingang 🔅 Einstellungen × 🖓 Abrufen 👻 🖋 Verfassen 🗿 Adressbuch 🛛 🛇 Schlagwörter 🗸 🖓 Schnellfilter Ξ ∨ 😭 crypto-al…osteo.net 🛠 🛛 🛛 Ungelesen 🕁 Gekennzeichnet 🖪 Kontakt 🛇 Schlagwörter 🛛 Anhang 🔎 Diese Nachrie 🕂 Neu Posteingang Anhänge * 0 Betref 00 Beteiliate Entwürfe Allgemein 🖈 Gesendet Bearbeiter Ъ ê Datenschutz Welcome to Posteo Posteo Support n Papierkorb Q Suchen ✓ 🚞 Local Folders Verfassen E-Mail-Inhalte 🖶 Drucken Entwürfe Datenschutz & Papierkorb 🖻 Speichern als Externe Inhalte in Nachrichten erlauben Ausnahmen... 🐼 Postausgang Sicherheit 🗊 Papierkorb leeren Erfahren Sie mehr über die Datenschutzaspekte externer Inhalte 🖵 Chat 📥 Add-ons M Konten-Einstellungen Webinhalte 🔅 Einstellungen 👔 ✓ Besuchte Webseiten und Links merken 🖌 Anpassen ✓ Cookies von Webseiten akzeptierer Ausnahmen. Datei Ansicht Cookies von Drittanbietern akzeptieren: Nie ~ Navigation Nachricht Behalten, bis: Thunderbird geschlossen wird Cookies anzeigen Extras Websites eine "Do Not Track"-Mitteilung senden, dass Ihre Online-Aktivitäten nicht verfolgt werden sollen ⑦ Hilfe 🖒 Beenden Passwörter Gespeicherte Passwörter... Thunderbird kann die Passwörter aller Ihrer Konten speichern Ein Master-Passwort schützt alle gespeicherten Passwörter, Sie müssen es aber einmal pro Sitzung eingeben. Master-Passwort verwenden Master-Passwort ändern... Junk Die folgenden Einstellungen gelten für alle Konten. In den Konten-Einstellungen können zusätzlich für jedes Konto Erweiterungen & getrennte Einstellungen vorgenommen werden Themes Wenn Nachrichten manuell als Junk markiert werden Ungelesen: 0 Gesamt: 2

(a) Klicke im Menü auf "Einstellungen"...

 $\rm (b)\dots$ und wähle anschließend links "Datenschutz & Sicherheit" aus. Setze einen Haken bei "Master-Passwort verwenden"

(a) Denk dir ein sicheres Passwort aus und bestätige mit "OK".



(b) Das Master-Passwort wurde gespeichert. Du musst es ab sofort beim Öffnen von Thunderbird ein Mal eingeben.



5 Einen öffentlichen Schlüssel importieren

Für Enigmail-Umsteiger*innen ändert sich hier nichts.

Wenn du einer Person eine verschlüsselte E-Mail schreiben möchtest, dann benötigst du den öffentlichen Schlüssel dieser Person. Bitte die Person, dir ihren öffentlichen Schlüssel per E-Mail zu schicken. In unserem Beispiel heißt die Person Bob.

Abbildung 10: Der öffentliche Schlüssel ist der E-Mail als Anhang angehängt.

(a) Klicke mit der rechten Maustaste auf den Anhang und wähle "OpenPGP-Schlüssel importieren".



Schlüssel überprüfen & akzeptieren 6

Achtung: Neu bei Thunderbird 78!

0

Bevor du einen Schlüssel nutzen kannst, musst du ihn einmalig akzeptieren. Das gilt für neue Schlüssel, nach dem Update auf Thunderbird 78 musst du aber einmalig auch alle gespeicherten Schlüssel akzeptieren! Das ist eingeführt worden, damit du jeden Schlüssel überprüfst, bevor du ihn verwendest. Mache dir dazu folgendes klar: Wenn eine Person, z.B. Bob, dir ihren öffentlichen Schlüssel per E-Mail schickt, kannst nicht ausschließen, dass jemand diese E-Mail abgefangen und Bobs Schlüssel ersetzt hat. Damit du überprüfen kannst, ob ein Schlüssel auch der richtige Schlüssel ist, hat jeder Schlüssel einen sogenannten "Fingerabdruck". Das ist eine lange Zeichenkette. Vergleiche mit Bob, ob der Fingerabdruck, der dir angezeigt wird, auch wirklich der Fingerabdruck von seinem Schlüssel ist! Verwende für diesen Vergleich einen anderen Kommunikationskanal, z.B. eine Signal-Nachricht oder ein persönliches Treffen, aber nicht E-Mail.

Du kannst den Schlüssel von Bob auch verwenden, ohne seinen Fingerabdruck zu überprüfen. Aber auch dann musst du Bob Schlüssel einmalig akzeptieren, bevor du Bob verschlüsselt schreiben kannst! Bobs E-Mails werden dann zukünftig als unsicher markiert.

Neue Schlüssel beim Importieren akzeptieren 6.1

Du kannst einen neuen Schlüssel direkt nach dem Importieren überprüfen und akzeptieren.

Abbildung 11: Bevor du einen Schlüssel nutzen kannst, musst du ihn akzeptieren.

(b) Überprüfe den Fingerabdruck und wähle die entsprechende Option aus. Bestätige mit "OK".



(c) Du kannst den Schlüssel auch akzeptieren, ohne den Fingerabdruck abzugleichen:

Wähle die entsprechende Option aus. Bestätige mit "OK".

Vorgeblicher Schli	isselbesitzer	Bob <crypto-bob@posteo.net></crypto-bob@posteo.net>									
Тур		öffentlicher Schlüssel									
Fingerabdruck		9171 E502 3A75 7CEA 5359 31CA 041F 4BC2 5807 F822									
Erzeugt am		11/08/2020									
Läuft ab am		11/08/2023									
Ihre Akzeptanz	Zertifizierun	gen Struktur									
Ihre Akzeptanz Akzeptieren Sie dies	Zertifizierun en Schlüssel für	gen Struktur das Verifizieren von digitalen Unterschriften und das Verschlüsseln	von								
Ihre Akzeptanz Akzeptieren Sie dies Nachrichten?	Zertifizierun en Schlüssel für	gen Struktur das Verifizieren von digitalen Unterschriften und das Verschlüsseln	von								
Ihre Akzeptanz Akzeptieren Sie dies Nachrichten? Akzeptieren Sie nur	Zertifizierun en Schlüssel für vertrauenswürd	gen Struktur das Verifizieren von digitalen Unterschriften und das Verschlüsseln ige Schlüssel. Verwenden Sie einen anderen Kommunikationskanal a	von Is E-Ma	3il							
Ihre Akzeptanz Akzeptieren Sie dies Nachrichten? Akzeptieren Sie nur um den Fingerabdrug	Zertifizierun en Schlüssel für vertrauenswürd ck des Schlüsse	gen Struktur : das Verifizieren von digitalen Unterschriften und das Verschlüsseln ige Schlüssel. Verwenden Sie einen anderen Kommunikationskanal a Is Ihres Kontakts zu verifizieren.	von Is E-Ma	3il							
Ihre Akzeptanz Akzeptieren Sie diese Nachrichten? Akzeptieren Sie nur um den Fingerabdruu Nein, diese	Zertifizierun en Schlüssel für vertrauenswürd ck des Schlüsse n Schlüssel zuri	gen Struktur das Verifizieren von digitalen Unterschriften und das Verschlüsseln ige Schlüssel. Verwenden Sie einen anderen Kommunikationskanal a Is Ihres Kontakts zu verifizieren. ickweisen.	von ils E-Ma	3il							
Ihre Akzeptanz Akzeptieren Sie diese Nachrichten? Akzeptieren Sie nur um den Fingerabdruc Nein, diese Nicht jetzt,	Zertifizierun en Schlüssel für vertrauenswürd ck des Schlüsse n Schlüssel zuri vielleicht späte	gen Struktur · das Verifizieren von digitalen Unterschriften und das Verschlüsseln ige Schlüssel. Verwenden Sie einen anderen Kommunikationskanal a Is Ihres Kontakts zu verifizieren. ickweisen. r	von ils E-Ma	ail							
Ihre Akzeptanz Akzeptieren Sie diese Nachrichten? Akzeptieren Sie nur um den Fingerabdruc Nein, diese Nicht jetzt, ja, aber ich	Zertifizierun en Schlüssel für vertrauenswürd ck des Schlüsse n Schlüssel zuri vielleicht späte habe nicht übe	gen Struktur · das Verifizieren von digitalen Unterschriften und das Verschlüsseln ige Schlüssel. Verwenden Sie einen anderen Kommunikationskanal a Is Ihres Kontakts zu verifizieren. ickweisen. r rprüft, dass es sich um den korrekten Schlüssel handelt.	von ils E-Ma	ail							

6.2 Gespeicherte PGP-Schlüssel akzeptieren

Als Enigmail-Umsteiger*in musst du einmalig alle gespeicherten Schlüssel akzeptieren!

Wenn du einen gespeicherten Schlüssel überprüfen und akzeptieren möchtest, kannst du dazu das Fenster "OpenPGP-Schlüssel verwalten" benutzen, das du vielleicht schon von Enigmail kennst.

Abbildung 12: Das Fenster "OpenPGP-Schlüssel verwalten" findet sich im Extras-Menü.

(a) Im Menü "Extras" auswählen…

(b) ..und anschließend "OpenPGP-Schlüssel verwalten" anklicken.

3	Р	osteingang - Mozilla Thunderbi	rd			3		Posteingang - Mozilla Thunderbir	ď		± - ¢ 😣
🖵 Abrufen 🔽 🖋 Verfasse	n 🖪 Adressbuch 🛇 Schlagwörter 🗸 🗌	∀ Schnellfilter			戸	♀ Abrufen ∨ Ø Verfasser	n 🖪 Adressbuch 🛇 Schlagwörter 🗸	Schnellfilter			E
Image: Constraint of the second s	P Adressbuch Schlagwörter ↓ Aungelesen ☆Gekennzeichnet → Betreff Posteo payment instructions Welcome to Posteo	osteingang - Mozilla Thunderbi Y Schnellfilter Akontakt Schlagwörter	rd Anhang P Diese Nachri Beteiligte Beteiligte Posteo Support Posteo Support Posteo Support	 Neu Anhànge Bearbeiten X Suchen Drucken Speichern als Papierkorb leeren Add-ons Konten-Einstellungen Ansacht Ansicht Ansicht Nachricht Extras Beenden 		 Abrufen < ✓ Verfasser ♀ crypto-alosteo.net ♀ Dotskingang Entwürfe ∢ Gesendet ♥ Papierkorb ♥ Dostausgang 	Adressbuch	Posteingang - Mozilla Thunderbir ▼ Schnellfilter et ▲Kontakt ∿Schlagwörter 15	d Anhang O Diese Nachri Bebelligte Bob Posteo Support Posteo Support	 Adressbuch Adressbuch Filter auf Ordner ar Filter auf Jachricht Junk-Filter auf Ordn Junk-Filter auf Ordn Junk-Filter auf Ordn Gespeicherte Date Importieren OgenPGP-Schlüssel Entwickler-Werkzet Neueste Chro S Aktivitäten Enigmail-Einstellun 	a - ♥ ♥ as Strg+Umschalt+B wwenden anwenden ner löschen ver anwenden ner löschen verwalten verwalten itrg+Umschalt+Entf gen migrieren
(r-4)				Ungelese	en: 0 Gesamt: 3	<u>6-0</u>				Unge	elesen: 0 Gesamt: 3

Hier werden dir alle gespeicherten Keys angezeigt: Alle deine Schlüssel (in fett) und alle öffentlichen Keys von anderen Personen. Mit einem Doppelklick kannst du dir den Fingerabdruck eines Schlüssels anzeigen lassen und den Schlüssel akzeptieren.

Abbildung 13: Über das Fenster "OpenPGP-Schlüssel verwalten" kannst du gespeicherte Schlüssel anzeigen und akzeptieren.

(a) Öffne den Schlüssel mit einem Doppelklick.

0			OpenPGP-Schlüss	el verwalten	≜ ø	8	
<u>D</u> atei	<u>B</u> earbeiten	<u>A</u> nsicht	<u>S</u> chlüsselserver	<u>E</u> rzeugen			
Nach	Schlüsseln sud	chen					
Nam Al Bo	e ice <crypto- bb <crypto-bol< td=""><td>alice@pos</td><td>steo.net> net></td><td>v</td><td>Schlüssel-ID 938802CDEB 041F48C25807</td><td>Läuft ab 11/08/2023 11/08/2023</td><td>E.</td></crypto-bol<></crypto- 	alice@pos	s teo.net> net>	v	Schlüssel-ID 938802CDEB 041F48C25807	Läuft ab 11/08/2023 11/08/2023	E.
						Schließ	len

(b) Überprüfe den Fingerabdruck und wähle die entsprechende Option aus. Bestätige mit "OK".

•	S	Schlüsseleigenschaften 🔺 🖉										
Vorgeblicher Schlüsselbe Typ	s itzer Bob < öffentl	Bob <crypto-bob@posteo.net> öffentlicher Schlüssel</crypto-bob@posteo.net>										
Fingerabdruck	9171 8	9171 E502 3A75 7CEA 5359 31CA 041F 4BC2 5807 F822										
Erzeugt am	11/08/	11/08/2020										
Läuft ab am	11/08/	2023										
Ihre Akzeptanz Zerti	izierungen	Struktur										
Akzeptieren Sie diesen Schlü Nachrichten?	ssel für das Ve	rifizieren von digitalen Unterschriften und das Verschlüsse	In von									
Akzeptieren Sie nur vertraue um den Fingerabdruck des S	nswürdige Sch chlüssels Ihres	üssel. Verwenden Sie einen anderen Kommunikationskan Kontakts zu verifizieren.	al als E	-Mail,								
🔵 Nein, diesen Schlüs	sel zurückweis	en.										
 Nicht jetzt, vielleich 	it später											
 Ja, aber ich habe ni 	cht überprüft,	lass es sich um den korrekten Schlüssel handelt.										
 Ja, ich selbst habe i 	iberprüft, dass	der Schlüssel über den korrekten Fingerabdruck verfügt.										
				ок 🖌								

(c) Du kannst den Schlüssel auch akzeptieren, ohne den Fingerabdruck abzugleichen. Wähle die entsprechende Option aus. Bestätige mit "OK".

The second se											
тур											
Fingerabdruck	9171 E502 3A75 7CEA 5359 31CA 041F 4BC2 5807 F822	9171 E502 3A75 7CEA 5359 31CA 041F 4BC2 5807 F822 11/08/2020									
Erzeugt am	11/08/2020										
Läuft ab am	11/08/2023										
Ihre Akzeptanz Akzeptieren Sie dieser Nachrichten? Akzeptieren Sie nur ve	Zertifizierungen Struktur Schlüssel für das Verifizieren von digitalen Unterschriften und das Verschlüss trauenswürdige Schlüssel. Verwenden Sie einen anderen Kommunikationska	seln von nal als E-Ma									
Ihre Akzeptanz Akzeptieren Sie dieser Nachrichten? Akzeptieren Sie nur ve um den Fingerabdruck	Zertifizierungen Struktur Schlüssel für das Verifizieren von digitalen Unterschriften und das Verschlüss trauenswürdige Schlüssel. Verwenden Sie einen anderen Kommunikationska des Schlüssels Ihres Kontakts zu verifizieren.	seln von nal als E-Ma									
Ihre Akzeptanz Akzeptieren Sie dieser Nachrichten? Akzeptieren Sie nur ve um den Fingerabdruck Nein, diesen	Zertifizierungen Struktur Schlüssel für das Verifizieren von digitalen Unterschriften und das Verschlüss trauenswürdige Schlüssel. Verwenden Sie einen anderen Kommunikationska des Schlüssels Ihres Kontakts zu verifizieren. ichlüssel zurückweisen.	seln von nal als E-Ma									
Ihre Akzeptanz Akzeptieren Sie dieser Nachrichten? Akzeptieren Sie nur ve um den Fingerabdruck Nein, diesen Nicht jetzt, v	Zertifizierungen Struktur Schlüssel für das Verifizieren von digitalen Unterschriften und das Verschlüss trauenswürdige Schlüssel. Verwenden Sie einen anderen Kommunikationska des Schlüssels ihres Kontakts zu verifizieren. Schlüssel zurückweisen. elleicht später	seln von nal als E-Ma									
Ihre Akzeptanz Akzeptieren Sie diesen Nachrichten? Akzeptieren Sie nur ve um den Fingerabdruck Nein, diesen Nicht jetzt, v Ja, aber ich h	Zertifizierungen Struktur Schlüssel für das Verifizieren von digitalen Unterschriften und das Verschlüss trauenswürdige Schlüssel. Verwenden Sie einen anderen Kommunikationska des Schlüssels Ihres Kontakts zu verifizieren. schlüssel zurückweisen. elicint später be nicht überprüft, dass es sich um den korrekten Schlüssel handelt.	seln von nal als E-Ma									

7 Eine verschlüsselte E-Mail schreiben

Für Enigmail-Umsteiger*innen gibt es kleine Neuerungen:

- Thunderbird kann nicht anhand der E-Mail-Adresse automatisch entscheiden, ob die E-Mail verschlüsselt werden soll oder nicht. Die Verschlüsselung ist standardmäßig einoder ausgeschaltet (siehe Einstellungen ändern) und kann für jede E-Mail manuell (de-)aktiviert werden.
- Thunderbird verschlüsselt immer auch den Nachrichten-Betreff.

Jetzt kannst du endlich eine verschlüsselte Nachricht an Bob schreiben! Vergiss nicht, deinen öffentlichen Schlüssel anzuhängen, damit Bob dir auch verschlüsselt anworten kann.

Abbildung 14: Verfasse eine Nachricht und klicke dann auf den kleinen Pfeil neben dem Feld "Sicherheit".

Hier kannst du die Verschlüsselung und die digitale Unterschrift (de-)aktivieren und deinen öffentlichen Schlüssel anhängen. Dass Verschlüsselung und digitale Unterschrift aktiviert sind, kannst du auch anhand der Schloss- und Siegel-Symbole in der Leiste unten rechts erkennen.

9	Verfassen: Re: Mein Key - Thunderbird									-	2	8	
<u>D</u> atei <u>B</u> earbeiten	<u>A</u> nsicht	<u>O</u> ptionen	Extras	<u>H</u> ilfe									
🖪 Senden 📔 🆧 Rechtschr. 🔽		Sicherh	🔒 Sicherheit 📉 🖬 Speichern 🗸								0 Anl	nang	•
Von	Alice <crv< td=""><td>Verschl</td><td>üsselűngs-</td><td>Technolog</td><td>gie</td><td>>,</td><td colspan="2">t 🗸 Kopie</td><td>e (CC)</td><td>Blindkoni</td><td>ie (BCC)</td><td>C)</td><td>»</td></crv<>	Verschl	üsselűngs-	Technolog	gie	>,	t 🗸 Kopie		e (CC)	Blindkoni	ie (BCC)	C)	»
7	Funce sery	O <u>N</u> icht ve	erschlüsse	In		_			. (,		- (2	-,	
An	crypto-bo	💿 Nur mit	<u>V</u> erschlüs	selung se	enden								
Bet <u>r</u> eff	Re: Mein K	🗹 Nachric	ht <u>u</u> ntersc	hreiben									
Diese Mail wird ver	schlüsselt	🗹 Meinen	öffentliche	en Schlüs	sel <u>a</u> nhäng	en							
Mein Schlüssel ist	im Anhang.	Sicherheitsinformationen anzeigen											
Am 11/8/20 um 2:12 > Im Anhang :)	₽M schrieb	Bob:											
							(DpenPGP	.0 ₽	Deutsch (Deuts	chla	nd)

Abbildung 15: Wenn du beim Senden der Nachricht diese Fehlermeldung bekommst, dann hast du entweder keinen Schlüssel von Bob (siehe Abschnitt Einen öffentlichen Schlüssel importieren) oder du hast Bobs Schlüssel noch nicht akzeptiert (siehe Abschnitt Schlüssel überprüfen & akzeptieren). Vielleicht kann Bob noch gar keine verschlüsselten E-Mails empfangen, dann zeige ihm doch, wie das geht! Du kannst natürlich auch die Verschlüsselung für diese Nachricht deaktivieren.



8 Eine Nachricht entschlüsseln

Für Enigmail-Umsteiger*innen ändert sich nur die Art der Darstellung.

Wenn du eine verschlüsselte E-Mail öffnest, wird diese automatisch entschlüsselt. Ob die Nachricht verschlüsselt ist und/oder eine digitale Unterschrift enthält, kannst du mit einem Klick auf "OpenPGP" oben rechts feststellen:

(a) Diese Nachricht ist verschlüsselt (achte auf das Schloss-Symbol) und wurde von Bob digital unterschrieben (Siegel-Symbol).



(b) Diese Nachricht ist zwar verschlüsselt und unterschrieben, du hast Bobs Fingerabdruck aber noch nicht überprüft!



(c) Diese Nachricht ist unverschlüsselt, aber von Bob unterschrieben.

