E-Mail mit OpenPGP verschlüsseln

Wir müssen kein Verschlüsselungsexperte sein, um verschlüsselte E-Mails, in meinem Beispiel mit dem Open Source Programm Thunderbird zu senden und zu empfangen. Mit dieser Anleitung zeige ich dir, wie du genau das tun kannst.

1. Thunderbird Installieren

Du benötigst **Thunderbird 78 oder neuer**, um dieser Anleitung zu folgen.

Windows und macOS

Lade dir Thunderbird herunter und installiere es auf deinem Computer.

Linux - Distributionen

Thunderbird ist in den meisten Fällen standardmäßig installiert.

2. Einrichten deines E-Mail-Kontos

Wenn du Thunderbird zum ersten Mal öffnest, wirst du automatisch durch den Prozess der Einrichtung deines E-Mail-Kontos geführt. In den meisten Fällen musst du nur deine bestehende E-Mail-Adresse und dein Passwort eingeben, und schon funktioniert es.

Du solltest überprüfen, dass der Ausgangsserver entweder auf Port 465 mit SSL/TLS oder Port 587 mit STARTTLS eingestellt ist.

3. Erstelle dir dein eigenes Schlüsselpaar

1. Klicke auf die Menüschaltfläche (≡) > **Kontoeinstellungen**.
2. Klicke im linken Menü auf **Ende-zu-Ende-Verschlüsselung**.
3. Klicke auf **Schlüssel hinzufügen**.
4. Stelle sicher, dass **Neuer OpenPGP-Schlüssel erzeugen** ausgewählt ist, und klicke dann auf **Weiter**.
5. Achte im nächsten Schritt, dass du unter **Identität** das richtige E-Mail Konto zum **erzeugen des neuen OpenPGP-Schlüssels** ausgewählt ist.
6. Unter **Ablaufdatum** kannst du nun unter **Schlüssel läuft ab in** zwischen **Jahren**, **Monaten**, **Tagen** und unter **Schlüssel läuft nicht ab** festlegen, ob oder wann dein erzeugter Schlüssel abläuft.
7. Die **erweiterte Einstellung** im gleichen Fenster ermöglicht dir noch den **Schlüsseltyp (RSA oder ECC)** wie auch die **Schlüsselgröße (3072 Bit oder 4096 Bit)** festzulegen.
8. Klicke auf **Schlüssel generieren** und warte, bis das neue Schlüsselpaar generiert wurde.
9. Klicke auf **Schließen**, sobald der Vorgang abgeschlossen ist.
10. Du bist nun bereit, E-Mails zu verschlüsseln!

Du kannst deinen Schlüssel jederzeit in den Einstellungen für die Ende-zu-Ende-Verschlüsselung (E2EE) verwalten oder einen neuen Schlüssel erstellen.

4. Bestehenden OpenPGP-Schlüssel importieren

Du kannst nun deine persönliche Schlüssel importieren, welche mit anderer OpenGPG-Software erzeugt wurden.

1. Klicke auf die Menüschaltfläche (≡) > **Kontoeinstellungen**.
2. Klicke im linken Menü auf **Ende-zu-Ende-Verschlüsselung**.
3. Klicke auf **Schlüssel hinzufügen**.
4. Klicke nun auf **Bestehenden OpenPGP-Schlüssel importieren**.

5. Klicke auf **Datei für den Import auswählen**.
6. Suche und wähle nun deinen schon persönlich, erstellen OpenPGP-Schlüssel aus.
7. Wenn du alles richtig gemacht hast und der OpenPGP-Schlüssel erfolgreich importiert wurde, bekommst du eine grün hinterlegte Bestätigung **Thunderbird erkannte einen importierbaren Schlüssel** angezeigt.
8. Mit einem Klick auf **Weiter** gelangst du zur **Eingabe** das von **dir bereits erstellten Passwortes für deinen persönlichen OpenPGP-Schlüssel**.
9. Gebe nun das **Passwort** ein und klicke auf **Weiter**.
10. Nun sollte eine grün hinterlegte Bestätigung **OpenPGP-Schlüssel wurde erfolgreich importiert** angezeigt werden.
11. Den **Importvorgang** schließt du mit einem Klick auf **Weiter** ab.

Um deinen importierten **OpenGPG-Schlüssel** für die E-Mail-Verschlüsselung zu verwenden, öffne die **Konten-Einstellungen** → **Ende-zu-Ende-Verschlüsselung** → unter **OpenGPG** den Schlüssel auswählen.

5. Importieren des öffentlichen Schlüssels eines Kontakts

Um eine verschlüsselte Nachricht zu versenden, benötigst du nicht nur dein eigenes Schlüsselpaar, sondern auch den öffentlichen Schlüssel des Empfängers. Lass uns einen importieren.

Als E-Mail-Anhang empfangene öffentliche Schlüssel

Wenn dir jemand seinen öffentlichen Schlüssel als E-Mail-Anhang schickt, bietet Thunderbird an, ihn für dich zu importieren.

Erkennen von öffentlich verfügbaren Schlüsseln

Manche Leute machen ihre öffentlichen Schlüssel per E-Mail durchsuchbar. Um dies zu überprüfen, öffnest du eine E-Mail von jemandem und klickst auf dessen E-Mail-Adresse. Klicke im Popup-Fenster auf **OpenPGP Key**.

Manuelles Importieren eines öffentlichen Schlüssels

Manche Leute veröffentlichen ihre öffentlichen Schlüssel auf einer Website oder einem Schlüsselserver. Einige sind direkt auf einer Website verfügbar, so dass jeder eine verschlüsselte Nachricht senden kann.

Hier beschreibe ich, wie du einen Schlüssel manuell in Thunderbird importieren kannst:

1. Lade den GPG-Schlüssel von deiner besuchten Website herunter (er befindet sich meistens in der Fußzeile einer Website).
2. Klicke nun in Thunderbird auf die Schaltfläche **Menü (m) > Kontoeinstellungen > Ende-zu-Ende-Verschlüsselung**.
3. Klicke auf die Schaltfläche **OpenPGP Schlüssel verwalten**.
4. Klicke im neuen Fenster auf **Datei > Öffentliche(n) Schlüssel aus Datei importieren**.
5. Wähle die heruntergeladene Datei aus.
6. Klicke auf **Öffnen** und dann auf **OK**.
7. Klicke im Pop-up-Fenster "Erfolg!" auf **OK**.
8. Du siehst nun die entsprechende E-Mail in der Liste der Schlüssel.
9. Um den Schlüssel zu verwenden, musst du bestätigen, dass du ihn akzeptieren und ihm vertrauen möchtest.
10. Führe dazu zunächst einen **Doppelklick** auf die Taste aus.
11. Wähle im Fenster Schlüsseleigenschaften eine der Optionen **Ja** und dann **OK > Schließen**.
12. Jetzt bist du bereit, verschlüsselte Nachrichten an den Anbieter der besuchten Website zu senden!

6. Sende und empfange verschlüsselte E-Mails

Jetzt kommt der spaßige Teil: heimlich kommunizieren! Hier erfährst du, wie du den Support-Team eine E-Mail schreiben und dein Anliegen ihnen sagen kannst.

1. Öffne Thunderbird und verfasse eine neue E-Mail.

2. Gebe nun die E-Mail Adresse des Supports in das Feld **An** ein.
3. Klicke auf das **Dropdown-Symbol** neben der Schaltfläche Sicherheit in der Symbolleiste.
4. Wähle **Verschlüsselung anfordern**. Dies wird automatisch Ihren öffentlichen Schlüssel an die E-Mail anhängen und den öffentlichen Schlüssel vom Support verwenden, den du zuvor importiert und verifiziert hast. Du kannst dies doppelt überprüfen, indem du auf die Schaltfläche **Sicherheit** klickst. Es sollte ein "ok"- Status neben dem Schlüssel vom Support angezeigt werden.
5. Verfasse die E-Mail fertig und sende sie ab!

Herzlichen Glückwunsch! Wiederhole einfach die Abschnitte 4 und 5, um mit allen anderen Benutzern der Verschlüsselung zu korrespondieren.

7. Sichere deine Schlüssel

Genauso wie du einen Ersatzschlüssel für dein Haus oder Wohnung hast, ist es wichtig, ein Backup deines Schlüsselpaares (öffentlicher und privater Schlüssel) zu haben.

Und so erstellst du dein Backup:

1. Klicke in Thunderbird auf die Schaltfläche **Menü (.5) > Kontoeinstellungen**.
2. Klicke im linken Menü auf **End-To-End-Verschlüsselung**.
3. Klicke rechts neben deinem persönliche Schlüssel auf das **Chevron-Symbol**, um weitere Informationen anzuzeigen.
4. Klicke auf **Mehr** und wähle dann **Öffentlicher Schlüssel exportieren** um deinen **öffentlichen Schlüssel** und das gleiche mit **Sicherheitskopie für geheimen Schlüssel erstellen** um deinen **privaten Schlüssel** zu sichern.
5. Speichere jeweils die beiden Dateien an einem sicheren Ort ab.