E-Mail-Verschlüsselung

Die wichtigsten Grundprinzipien:

- Bei asymmetrischer Verschlüsselung hat **jede Partei ein persönliches Schlüsselpaar**, einen **öffentlichen** und einen **privaten** Schlüssel. Was mit einem dieser Schlüssel verschlüsselt wird, kann nur mit dem anderen entschlüsselt werden.
- Die Sicherheit des Verfahrens hängt von zwei Annahmen ab:
  - private Schlüssel können von niemand sonst benutzt werden
    → private Schlüssel sichern mit Passphrasen, nicht weitergeben
  - öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet
    → absichern durch Fingerabdruck-Abgleich, mehrere Kanäle, Web of Trust
- Es gibt zwei Aktionen, die unabhängig voneinander eingesetzt werden können:
  - Nachricht **verschlüsseln** – mit dem **öffentlichen Schlüssel des Empfängers**
    → Vertraulichkeit: Nachricht kann nur mit privatem Schlüssel der E. gelesen werden
  - Nachricht kryptografisch **signieren** – mit dem **privaten Schlüssel der Absenderin**
    → Integrität und Authentizität: mit öffentlichem Schlüssel des A. kann geprüft werden, dass die Nachricht nicht verändert wurde und dass niemand anderes sie schrieb
- Wenn ein privater Schlüssel verlorengeht, können Nachrichten nicht mehr entschlüsselt werden → das Thunderbird-Profil datensichern[1], auch hier an Verschlüsselung denken (via Passphrase für private Schlüssel oder besser separat für die gesamte Sicherung)

Schritt 1: Software installieren – Mozilla Thunderbird

Seit **Version 78.2** ist PGP ein direkter Bestandteil von Thunderbird. Ältere Anleitungen, bei denen zusätzlich GnuPG und das Thunderbird-Add-on Enigmail zu installieren waren, gelten nicht mehr. Es gibt zwar noch eine Version von Enigmail (2.2.x) in Thunderbird 78+, diese hat aber nur einen Zweck: Die Übernahme von Schlüsseln und Einstellungen aus einer älteren Installation von Thunderbird (mit GnuPG und Enigmail).

- Thunderbird installieren und starten
  - https://www.thunderbird.net/de/
  - Beim ersten Aufruf E-Mail-Konto konfigurieren und Feineinstellung durchführen (S. 6)
- Stelle sicher, dass in Thunderbird ein Hauptpasswort (Master-Passwort) eingestellt ist: ≡ **Menübutton** → ***Extras*** → ***Einstellungen*** klicken, dann unter ***Datenschutz & Sicherheit*** unter ***Passwörter***, falls noch nicht geschehen, das Hauptpasswort aktivieren (Master-Passwort verwenden) und ein (starkes) Passwort zweimal eingeben. Bei jedem Start wird dich Thunderbird nun nach diesem Passwort fragen, aber nur einmal. Das Hauptpasswort sichert evtl. gespeicherte Passwörter zu deinen Mail-Konten, Kalendern etc. und auch (seit Version 78) deine privaten PGP-Schlüssel.

---

[1] Zu sicherndes Verzeichnis, jeweils relativ zum persönlichen „Stammverzeichnis“:
• Windows: ***Application Data\Roaming\Thunderbird*** • macOS und Linux: ***.thunderbird***

Das Thunderbird-Profil kann sehr viel Speicherplatz beanspruchen, wenn Mails heruntergeladen (POP) oder synchronisiert (IMAP) werden. Empfehlung: Unterverzeichnisse namens *ImapMail* von der Datensicherung ausschließen.

Genau genommen enthält das oben genannte Verzeichnis nur eine Datei *profiles.ini*, die angibt, wo die Profie gespeichert sind (es kann mehrere geben). Das eigentliche Profil ist in der Regel ein Unterverzeichnis davon. Um den genauen Ort zu finden: ≡ **Menübutton** → ***Hilfe*** → ***Informationen zur Fehlerbehebung*** öffnen. Im Abschnitt *Allgemeine Informationen* findet sich der Punkt *Profil-Verzeichnis*, daneben ist ein Knopf, um das Verzeichnis zu öffnen.

Schlüssel und Einstellungen von einer alten Installation übernehmen

Thunderbird 78+ verwendet nicht mehr denselben „Schlüsselvorrat“ wie das systemweit installierte GnuPG. Die Schlüssel werden jetzt in den Thunderbird-Einstellungen (im „Profil“) gespeichert. Wenn du bereits mit einer früheren Version von Thunderbird gearbeitet hast oder mit einer anderen Software, die GnuPG-Schlüssel verwendet, kannst du diese Schlüssel in Thunderbird 78+ übernehmen:

- ≡ **Menübutton** → ***Add-ons*** aufrufen und, falls nötig, zu *Erweiterungen* wechseln. Ist Enigmail bereits als Erweiterung vorhanden?
  - Ja: zur Sicherheit über das Zahnradsymbol alle Erweiterungen aktualisieren
  - Nein: Ins Suchfeld „Enigmail“ eingeben, Enigmail in der Ergebnisliste finden und zu Thunderbird hinzufügen, Reiter mit den Suchergebnissen wieder schließen
- den Reiter mit den Add-ons schließen und über ≡ **Menübutton** → ***Extras*** → ***Enigmail-Einstellungen migrieren*** die Migration starten, danach den entstandenen Reiter „Abschied von Enigmail“ schließen.

Schritt 2: Schlüssel erstellen

- Stelle sicher, dass du ein Hauptpasswort verwendest (→ Schritt 1, zweiter Punkt).
- In Thunderbird ≡ **Menübutton** → ***Extras*** → ***OpenPGP-Schlüssel verwalten*** klicken
  - Die **Schlüsselverwaltung** ist ein eigenes Fenster, in dem sowohl deine eigenen *Schlüsselpaare* (öffentlicher und privater Schlüssel) als auch die Schlüssel deiner Kommunikationspartner (nur öffentliche Schlüssel) zu sehen sind. Letztere können über den Menüpunkt ***Ansicht*** → ***Schlüssel anderer Personen anzeigen*** ein- und ausgeblendet werden. Schlüsselpaare werden fett dargestellt.
  - Falls du noch kein eigenes Schlüsselpaar hast, kannst du es hier erzeugen über den Menüpunkt ***Erzeugen*** → ***neues Schlüsselpaar***. Wir empfehlen Schlüsseltyp RSA und die größte Schlüssellänge, 4096 Bit. Ein Ablaufdatum zu setzen, ist eine empfehlenswerte Vorsichtsmaßnahme. Die Ablauffrist kann später verlängert werden.
  - Vorsicht beim Löschen alter Schlüsselpaare: Damit werden die Mails, die mit diesem privaten Schlüssel entschlüsselt werden müssten, unlesbar. Wenn du eines deiner Schlüsselpaare nicht mehr verwenden willst, kannst du es doppelklicken und den Punkt „Nein, nicht als meinen persönlichen Schlüssel verwenden“ anwählen. Wenn du sicher bist, dass eines deiner Schlüsselpaare nicht mehr gebraucht wird (vielleicht wurde es nur testweise erzeugt und verwirrt jetzt nur noch), kannst du es löschen.

Überprüfe in den Kontoeinstellungen, ob der richtige private Schlüssel verwendet wird und ob andere Einstellungen stimmen:

- Klicke in Thunderbird ≡ **Menübutton** → ***Konten-Einstellungen***
- Wähle das E-Mail-Konto, für das die Schlüssel gelten sollen, und klicke dort den Unterpunkt ***Ende-zu-Ende-Verschlüsselung*** an. Überprüfe, dass ein OpenPGP-Schlüssel für dieses Konto bekannt und ausgewählt ist. Dieser muss zur E-Mail-Adresse dieses Kontos passen. Weiter unten findet sich der Punkt ***Senden von Nachrichten – Standardeinstellungen***. Hier sollte die Verschlüsselung standardmäßig nicht aktiviert sein. Sonst weigert sich Thunderbird, Mails zu senden, wenn du zu einer Empfangsadresse keinen akzeptierten Schlüssel hast.

Schritt 3: öffentliche Schlüssel importieren/exportieren

Zum Verschlüsseln wird der öffentliche Schlüssel des Empfängers verwendet. Also: Damit andere Personen dir verschlüsselte E-Mails schicken können, brauchen sie deinen öffentlichen PGP-Schlüssel.

Key-Server sind die bequemste Möglichkeit, öffentliche Schlüssel zu verteilen. Bedenke, dass die im Schlüssel eingetragenen E-Mail-Adressen dann öffentlich sind. Früher haben Key-Server einen öffentlichen Schlüssel ohne weitere Prüfung angenommen. Dies hat zu mehreren Problemen geführt und ist inzwischen überholt. Thunderbird 78+ unterstützt nur noch das Herunterladen vom Server keys.openpgp.org. Keys dort hochzuladen, erfordert einen menschlichen Eingriff (Reaktion auf eine Bestätigungs-Mail), deshalb gibt es seit dem Ende von Enigmail keinen einfachen Klickweg zum Hochladen deines Schlüssels.

- Klicke in Thunderbird: ≡ **Menübutton** → ***Extras*** → ***OpenPGP-Schlüssel verwalten***
- **Rechtsklick** auf deinen Schlüssel, wähle ***Schlüssel in Datei exportieren*** (nur der öffentliche Schlüssel ist gemeint)
- Besuche keys.openpgp.org/upload mit dem Browser deiner Wahl, lade die gerade gespeicherte Schlüsseldatei dort hoch
- Klicke auf „Send Verification Email“, klicke auf den Link in der Bestätigungs-Mail

Oder den öffentlichen Schlüssel direkt an Kommunikationspartner schicken:

- Klicke in Thunderbird: ≡ **Menübutton** → ***Extras*** → ***OpenPGP-Schlüssel verwalten***
- **Rechtsklick** auf deinen Schlüssel, ***Öffentliche Schlüssel per E-Mail senden***
- Mail normal ausfüllen (Empfänger, Betreffzeile, Text) und absenden
- Oder: Mail verfassen, ***Optionen*** → ***Meinen öffentlichen Schlüssel anhängen*** anhaken

Um anderen Personen verschlüsselte Nachrichten zu schreiben, brauchst du wiederum deren öffentlichen PGP-Schlüssel.

Auf Key-Server suchen:

- In einer Mail Rechtsklick auf z.B. die Absenderin, ***OpenPGP-Schlüssel suchen***
- Alternative: klicke ≡ **Menübutton** → ***Extras*** → ***OpenPGP-Schlüssel verwalten***, dann ***Schlüsselserver*** → ***Schlüssel online finden***, um einzelne Schlüssel mit einer Suche nach der E-Mail-Adresse zu finden

Oder Schlüssel aus E-Mail-Anhang importieren:

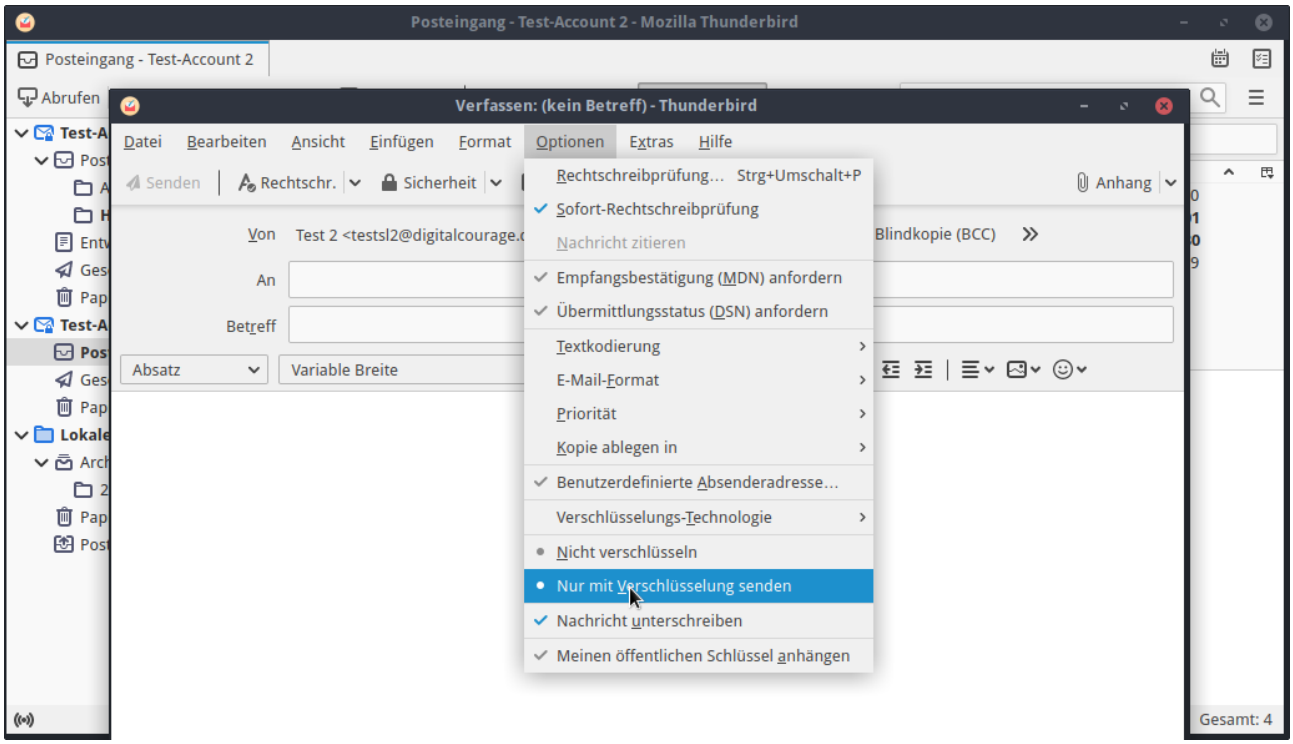
- Der PGP-Schlüssel hat die Dateiendung .asc
- Rechtsklick auf den Anhang: ***OpenPGP-Schlüssel importieren***, im folgenden Dialog die Option Akzeptiert (nicht verifiziert) wählen, wenn du den Schlüssel nutzen möchtest

Oder Schlüssel zum Beispiel von einer Website herunterladen und speichern, dann

- ≡ **Menübutton** → ***Extras*** → ***OpenPGP-Schlüssel verwalten*** öffnen
- Dort im Menü ***Datei*** → ***Öffentliche(n) Schlüssel aus Datei importieren*** wählen
- Manchmal kann der Schlüssel aus einer exteren Quelle auch in die Zwischenablage kopiert werden, dann ***Bearbeiten*** → ***Schlüssel aus Zwischenablage importieren***

Bei jedem Importvorgang bekommst du einen Dialog, der dir anbietet, den Fingerprint des Schlüssels mit der anderen Person zu vergleichen. Nutze dies, soweit möglich.

Schritt 4: E-Mails unterschreiben und verschlüsseln



- Verfasse eine neue E-Mail in Thunderbird.
- Entscheide, ob du die Optionen ***Nur mit Verschlüsselung senden*** und ***Nachricht unterschreiben*** aktivierst. Du erreichst sie auch über den Pfeil neben dem Knopf ***Sicherheit***.
  - Verschlüsseln setzt voraus, dass der Empfänger auch PGP nutzt.
  - **Unterschreiben verwendet den privaten Schlüssel der Absenderin**, ist also immer möglich – die Signatur ist ein Zusatz zu deiner Mail, der Empfänger kann sie prüfen oder ignorieren. Es ist auch möglich und eventuell sinnvoll, nur zu unterschreiben, ohne zu verschlüsseln. Durch die Unterschrift kann nachgewiesen werden, dass die Mail von dir kam und nach dem Absenden nicht verändert wurde.
- Wenn du deinen Schlüssel als Mail-Anhang weitergeben möchtest, die Option „Meinen öffentlichen Schlüssel anhängen“ wählen.
- Nicht selten wird Thunderbird sich weigern, deine Mail abzusenden, mit der Meldung „Die Nachricht kann nicht mit Ende-zu-Ende-Verschlüsselung gesendet werden, weil es Probleme mit den Schlüsseln folgender Empfänger gibt“. Das weist darauf hin, dass du zu der Adresse (zu einiger der Adressen), an die du schreiben möchtest, den öffentlichen Schlüssel entweder gar nicht kennst oder ihn nicht akzeptiert hast.
  - Nach Schließen dieser Meldung öffnet sich der Dialog „Sicherheit OpenPGP-Nachricht“, der dir anzeigt, welcher Schlüssel welches Problem hat. Du kannst fehlende Schlüssel im Key-Server suchen oder schon vorhandene Schlüssel akzeptieren.
  - Wenn das nicht funktioniert, musst du das Absenden der Mail abbrechen und a) die Schlüssel auf anderen Wegen suchen oder b) die Liste der Empfangsadressen ändern oder c) dich entscheiden, dass du diese Mail doch nicht verschlüsselst.

Bonusmaterial I: Vertrauen in Schlüssel aufbauen

Eine der zwei Grundbedingungen vom Anfang lautete: „öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet“. Diese Aufgabe wird meist gelöst, indem wir unser Vertrauen verlagern auf Mittels-Personen oder -Institutionen, die hoffentlich gut prüfen können, welcher Schlüssel zu welcher Identität gehört – wir bauen eine Vertrauenskette.

Web of Trust statt institutionalisierten Zertifizierungsstellen

Zur Philosophie von PGP gehört der Aufbau von Vertrauensketten nach dem Prinzip des „Web of Trust“. Das ist ein ‚Graswurzelprinzip‘, ein Gegenentwurf zu den meisten Umsetzungen von X.509 (der Grundlage von SSL/TLS und damit von HTTPS), wo das Vertrauen auf ausgewählten, im Vorhinein festgelegten Zertifizierungsstellen basiert und das von ihnen ausgesprochene Vertrauen zu einer Ware wird. Im Web of Trust kannst du selbst öffentliche PGP-Schlüssel von anderen zertifizieren (mit ihrem Schlüssel unterschreiben). Damit bestätigst du die Zuordnung des Schlüssel zu dieser Person. So entsteht ein „Vertrauensnetzwerk“ (Web of Trust): Wer die andere Person nicht kennt, aber dich kennt und dir vertraut, kann auch dem Schlüssel der anderen Person vertrauen. Allerdings wird über diese Unterschriften auch ein Teil deines Kontakt-Netzwerks bekannt.

Thunderbird 78+ setzt auf indivuelle Einstellungen

Weil das Web of Trust in der Anwendung kompliziert ist und die Vertrauenswürdigkeit der Mittels-Personen schwer geprüft werden kann, hat es sich nie weit verbreitet. Im neuen Thunderbird wird es derzeit gar nicht unterstützt. Jeden Schlüssel, den du verwenden willst, musst du vorher als „akzeptiert“ markieren. Beim Import von neuen Schlüsseln kannst du das direkt auswählen – wenn du aber einen alten Schlüsselvorrat migriert hast, musst du jeden einzelnen Schlüssel bei der ersten Verwendung akzeptieren.

Aber wie kannst du ohne Zertifizierungen vertrauen, dass du die richtigen Schlüssel hast? Das geht durch Vergleich von Fingerprints im direkten Kontakt oder durch die Nutzung von mehreren möglichst unabhängigen Kanälen, um das Risiko einer Verfälschung zu minimieren. Den Fingerprints kannst du bei jedem Import vergleichen (Thunderbird zeigt ihn an), wenn du parallel dazu einen direkten Kontakt herstellen kannst. Unabhängige Kanäle könnten sein: persönliche Mails, Key-Server, Schlüssel oder Fingerprint auf der persönlichen Website, Postings in Foren oder sozialen Medien, Visitenkarten u. ä.

Bonusmaterial II: Feineinstellung

Eine Sammlung von empfohlenen Veränderungen in ≡ **Menübutton** → ***Einstellungen***

- Keine Webseite in leeren Vorschaufenstern: Reiter ***Allgemein***, ganz oben keinen Haken bei ***Beim Aufrufen von Thunderbird die Startseite anzeigen***
- Mails nicht sofort als gelesen markieren, wenn sie im Vorschaufenster erscheinen: Unter ***Lesen & Ansicht*** wechseln zu ***Nach dem Anzeigen für … Sekunden*** (z.B. 5s)
- Speicherplatz reduzieren: Weil Thunderbird auch Webseiten anzeigen kann, hat es auch einen Cache. Der wird zu selten genutzt, um nützlich zu sein. Unter ***Speicherplatz*** kannst du den Cache ***Jetzt leeren*** und via ***Automatisches Cache-Management ausschalten*** die Cache-Größe auf 0 MB reduzieren.
- Konfiguration bearbeiten: ≡ **Menübutton** → ***Einstellungen*** → Icon ***Allgemein*** → ganz unten Knopf ***Konfiguration bearbeiten …*** klicken und
  - JavaScript deaktivieren: **javascript** ins Suchfeld eingeben, Einstellung **javascript.enabled** finden; falls **true**, per Doppelklick auf **false** setzen

    JavaScript ist nie in Mails aktiviert, aber Thunderbird kann auch normale Webseiten anzeigen. Die häufigste Anwendung ist das Installieren von Add-ons. Die dafür verwendeten Webseiten benötigen JavaScript. Ohne JavaScript kannst du die Anwendungen nur herunterladen und speichern. Dann kannst du aber ≡ **Menübutton** → ***Add-ons*** öffnen und die heruntergeladenen Dateien (Endung .xpi) dort hineinziehen.
  - Falls gewünscht, dafür sorgen, dass neue Mails oben stehen: **sort_order** ins Suchfeld eingeben, die beiden mit **mailnews** beginnenden Einträge doppelklicken, Wert **2** eingeben, Enter (wirkt nur für Mail-Ordner, die noch nicht geöffnet wurden)
- Datenschutz-Einstellungen: Es gibt keinen Anlass, in Thunderbird Cookies zu akzeptieren oder Besuchte Webseiten und Links zu merken. Unter ***Datenschutz & Sicherheit*** kann dies ausgeschaltet werden. Auch die ***Datenerhebung durch Thunderbird*** kannst du deaktivieren.