

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 **öffentlichem Schlüssel der Empfängerin**
→ Vertraulichkeit: Nachricht kann nur mit privatem Schlüssel der E. gelesen werden
 - Nachricht kryptografisch signieren – mit dem **privaten Schlüssel des Absenders**
→ 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 → GnuPG-Schlüsselringe datensichern¹, auch hier an Verschlüsselung denken (via Passphrase für private Schlüssel oder separat für die gesamte Sicherung)

Schritt 1: Software installieren – GnuPG, Thunderbird und Enigmail

1. GnuPG zur Verschlüsselung der E-Mails.

- Linux: meistens schon installiert
- Windows: GPG4Win <https://www.gpg4win.org/> (alle Komponenten installieren)
- macOS: GPGTools <https://gpgtools.org/>

2. E-Mail-Programm Thunderbird zur Verwaltung der E-Mails.

- <https://www.thunderbird.net/de/>
- Beim ersten Aufruf E-Mail-Konto konfigurieren und Feineinstellung durchführen (S. 4)

3. Thunderbird-Add-On Enigmail, die Schnittstelle zu GnuPG.

- In Thunderbird unter ≡ **Menübutton** → **Add-Ons** links auf „Erweiterungen“ klicken und dann in der Suchleiste oben rechts nach Enigmail suchen und installieren („zu Thunderbird hinzufügen“).
- Die Software p≡p („Junior Mode“) noch nicht verwenden. Falls in Thunderbird über den ≡ **Menübutton** der Unterpunkt **Enigmail/p≡p** → **Einstellungen** zu finden ist: diesen aufrufen, in den Reiter „Kompatibilität“ gehen, „Nutzung von S/MIME und Enigmail erzwingen“ auswählen und schließen. Anschließend in ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten** nachsehen, ob gerade von p≡p ein Schlüsselpaar erzeugt worden ist (aktuelles Datum, keine Passphrase – zum Test Widerrufszeugnis erzeugen). Falls dieser Schlüssel wirklich neu ist, also noch nicht verwendet wurde, sollte er gelöscht werden, sonst deaktiviert.
Falls nur der Menüpunkt **Enigmail** (ohne p≡p) vorkommt, diesen Schritt überspringen.

¹ Zu sicherndes Verzeichnis, jeweils relativ zum persönlichen „Stammverzeichnis“:

• Windows: **Application Data\Roaming\GnuPG** • macOS und Linux: **.gnupg**

Schritt 2: Schlüssel erstellen

Mit dem Assistenten:

- In Thunderbird über den ≡ **Menübutton** → **Enigmail** → **Einrichtungsassistent** auswählen
 - Tipp: Lies die Texte des Assistenten in Ruhe durch.
- Wähle die **ausführliche Konfiguration** für Fortgeschrittene.
- Wähle „Ich möchte ein neues Schlüsselpaar erzeugen“.
- Gib eine **Passphrase** ein.
 - Diese musst du immer eingeben, wenn du auf den Schlüssel zugreifen willst, um Missbrauch des Schlüssels zu verhindern. Du kannst sie später ändern.
- Schlüssel wird erzeugt, dies kann eine Weile dauern.
- Erzeuge das **Widerrufszertifikat** (jederzeit wiederholbar, solange du deinen privaten Schlüssel und dessen Passphrase hast).
 - Damit kannst du deinen öffentlichen Schlüssel von Key-Servern widerrufen, auch nach Verlust des privaten Schlüssels (oder der Passphrase).

Oder manuell:

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- Dann **Erzeugen** → **Neues Schlüsselpaar**
- Wähle das E-Mail-Konto, für das die Schlüssel gelten sollen
- Gib eine **Passphrase** ein
- Ablaufdatum nicht länger als 5 Jahre
- Unter Erweitert: Schlüsselstärke **4096** Bit, Algorithmus RSA
- Schlüssel erzeugen, dies kann eine Weile dauern
- Erzeuge das **Widerrufszertifikat**

Schritt 3: öffentliche Schlüssel importieren/exportieren

Zur Verschlüsselung verwendet man den **öffentlichen Schlüssel der Empfängerin**. Also: Damit andere Personen dir verschlüsselte E-Mails schicken können, brauchen sie deinen öffentlichen PGP-Schlüssel.

Den öffentlichen Schlüssel auf Key-Server hochladen:

Key-Server sind die bequemste Möglichkeit. Dort kann dein Schlüssel einfach gefunden werden, allerdings sind die im Schlüssel eingetragenen E-Mail-Adressen dann öffentlich.

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- Setze einen Haken bei **Standardmäßig alle Schlüssel anzeigen**
- **Rechtsklick** auf deinen Schlüssel, auf Schlüsselserver hochladen

Oder den öffentlichen Schlüssel direkt an Kommunikationspartner schicken:

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**

- **Rechtsklick** auf deinen Schlüssel, **Öffentliche Schlüssel per E-Mail senden**

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

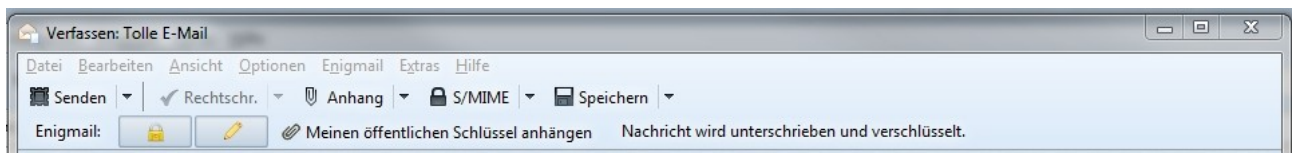
Auf Key-Server suchen:

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- Dann **Schlüsselserver** → **Schlüssel suchen**, um einzelne Schlüssel zu finden
- Oder **Schlüsselserver** → **Schlüssel für alle Kontakte suchen** (damit gibst du allerdings dem Key-Server dein Kontakt-Netzwerk bekannt)

Oder Schlüssel aus E-Mail-Anhang importieren:

- Der PGP-Schlüssel hat die Dateiendung .asc
- Rechtsklick auf die Datei: PGP-Schlüssel importieren.

Schritt 4: E-Mails unterschreiben und verschlüsseln



- Neue E-Mail in Thunderbird verfassen
- Stelle sicher, dass **unterschreiben** und **verschlüsseln** aktiviert ist
 - Verschlüsseln setzt voraus, dass der Empfänger auch PGP nutzt.
 - Unterschreiben geht immer – auch wenn Empfänger nichts damit anfangen können. Es ist auch möglich und evtl. sinnvoll, nur zu unterschreiben, ohne zu verschlüsseln.
- Zum Unterschreiben muss du beim Senden deine **Passphrase** eingeben
- Ggf. im Menü unter Enigmail die Option „Meinen öffentlichen Schlüssel anhängen“ wählen.

Bonusmaterial I: Schlüssel unterschreiben (Key-Signing)

Du kannst öffentliche PGP-Schlüssel von anderen Leuten 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 dadurch möglicherweise dein Kontakt-Netzwerk auf einem Key-Server öffentlich einsehbar. Überlege dir also, wessen Keys du signierst.

Überprüfe, ob der besagte Schlüssel zu der Person gehört:

- Wenn ihr Name in der E-Mail-Adresse vorkommt: prüfe z.B. per Personalausweis
- Sonst: lasse dir von ihr eine verschlüsselte und unterschriebene E-Mail schicken mit einem Inhalt, den du dir im direkten Kontakt ausdenkst und mitteilst.

Gleiche den Schlüssel-Fingerabdruck ab:

Als erstes überprüfst du, ob der Schlüssel, den die andere Person besitzt, dem öffentlichen Schlüssel entspricht, den du von ihr hast. Dies geht über den weltweit eindeutigen Fingerabdruck.

- Lasse dir den öffentlichen Schlüssel per Mail schicken oder lade ihn vom Key-Server
- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → **Schlüsseleigenschaften**
- Lasse dir von der anderen Person den Fingerabdruck ihres Schlüssel geben – ausgedruckt auf Papier (z.B. Visitenkarte) oder diktieren etc.

Schlüssel unterschreiben

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → **Unterschreiben**
- Zum Signieren musst du deine **Passphrase** eingeben

Den signierten Schlüssel seinem Besitzer schicken:

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → öffentlicher Schlüssel per E-Mail senden

Wenn jemand anderes deinen Schlüssel signiert hat und dir schickt, kannst du ihn auf einen Keyserver hochladen, wenn du möchtest. Falls dein Schlüssel dort schon liegt, wird er aktualisiert.

Unterschriften einsehen:

- Wähle in Thunderbird: ≡ **Menübutton** → **Enigmail** → **Schlüssel verwalten**
- **Rechtsklick** auf den Schlüssel → **Schlüsseleigenschaften** → Reiter **Zertifizierungen**

Bonusmaterial II: Feineinstellung

- Einstellungen in Thunderbird korrigieren: ≡ **Menübutton** → **Einstellungen** → **Icon „Erweitert“** → Reiter **Allgemein** → Knopf **Konfiguration bearbeiten ...** und
 - JavaScript deaktivieren: **javascript** ins Suchfeld eingeben, Einstellung **javascript.enabled** finden; falls **true**, per Doppelklick auf **false** setzen
 - 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)
- Eine Einstellung nach der Installation von Enigmail, ohne die manche Mails nicht entschlüsselt werden:
 - ≡ **Menübutton** → **Add-Ons** → im Fenster links **Erweiterungen** → bei **Enigmail** den Knopf **Einstellungen** klicken
 - Falls Reiter **Erweitert** nicht vorhanden, im Reiter **Allgemein** den Knopf **Experten-Optionen und -Menüpunkte anzeigen** klicken
 - Reiter **Erweitert** → Haken entfernen bei **Anhänge nur herunterladen, wenn diese geöffnet werden sollen (nur bei IMAP)**
 - falls gewünscht, wieder zurück zum Reiter **Allgemein** und Knopf **Experten-Optionen und -Menüpunkte ausblenden** klicken
 - Einstellungen mit **OK** schließen