

E-Mails per PGP verschlüsseln

E-Mail-Verschlüsselung Einrichten

Wenn du eine E-Mail an z.B. legal@letztegeneration.org schickst, dann kannst du diese vor dem Abschicken auf deinem Gerät verschlüsseln. So können dein und unser Mailprovider sowie dein und unser Internetprovider nicht mitlesen.

Diese Anleitung erklärt wie die PGP-Verschlüsselung für den E-Mail-Anbieter [ProtonMail](#) oder den E-Mail-Client [Thunderbird](#) eingerichtet werden kann.

“ **ProtonMail** ist ein Anbieter mit dem man direkt im Browser PGP-verschlüsselte E-Mails senden und empfangen kann. ProtonMail ist relativ einsteigsfreundlich und kann **für deine private E-Mail-Adresse** verwendet werden, um damit verschlüsselt mit AGs/WiGs zu kommunizieren.

“ PGP-Verschlüsselung funktioniert aktuell nicht mit unserem [Webmail](#).

“ Wenn du bei einem **anderen Anbieter** bist oder mit deiner **AG/WiG-Adresse** verschlüsselte E-Mails senden und empfangen willst, brauchst du einen E-Mail-Client mit PGP-Unterstützung wie z.B. **Thunderbird**.

Die Anleitung behandelt folgende Themen (jeweils für ProtonMail und Thunderbird):

- PGP-Verschlüsselung einrichten: Schlüsselpaar erzeugen und öffentlichen Schlüssel verbreiten
- Öffentlichen Schlüssel importieren (brauchst du, um an diese E-Mail eine verschlüsselte Nachricht zu schicken)
- Nur Thunderbird: Es existiert bereits ein Schlüsselpaar, z.B. von deiner AG/WiG (du bekommst privaten und öffentlichen Schlüssel, die du importieren möchtest)

Bei Fragen wende dich bitte an die IT-AG: it-support@letztegeneration.org.

ProtonMail

“ ProtonMail ist zwar sehr einsteigsfreundlich, aber aufgrund der webbasierten Architektur nicht so sicher wie ein nativer E-Mail-Client mit PGP-Verschlüsselung wie z.B. Thunderbird.

PGP-Schlüsselpaar erzeugen

ProtonMail generiert automatisch ein Schlüsselpaar für deinen Account.

Unter <https://account.proton.me/u/0/mail/encryption-keys> kannst du deinen Schlüssel sehen.

Schlüssel veröffentlichen

Wenn du anderen Menschen das Hinzufügen deines Schlüssel erleichtern willst, dann lade deinen **öffentlichen** Schlüssel bei keys.openpgp.org hoch.

Dazu [hier](#) deinen Schlüssel exportieren und auf <https://keys.openpgp.org/upload> hochladen. Klicke auf "verifizieren" und auf den Link in der E-Mail.

Öffentlichen Schlüsseln importieren

Bei ProtonMail muss der öffentliche Schlüssel der:des Empfängerin:Empfängers im Adressbuch hinterlegt werden. So geht es:

1. In die Weboberfläche einloggen, bis du deinen Posteingang siehst.
2. Oben rechts auf das Kontakte Icon mit den 2 Köpfen klicken:

ProtonMail-Adressbuch

1. nach legal@letztegeneration.org suchen beziehungsweise diese Adresse anlegen.
2. Den Kontakt öffnen und auf das Zahnrad klicken.
3. Erweiterte PGP-Einstellungen einblenden.
4. Den öffentlichen Schlüssel hier herunterladen:
 - AGs und WiGs: pgp.letztegeneration.org/
 - [Umwelt-Treuhandfond](#)

- restliche Welt: <https://keys.openpgp.org>

5. den öffentlichen Schlüssel in ProtonMail wieder hochladen (im Bild rot 1.).
6. die Verschlüsselung immer aktivieren „E-Mails verschlüsseln“ (im Bild rot 2.).

Nun sollte es so aussehen (nur mit [letztegeneration.org](https://keys.openpgp.org) statt [letztegeneration.de](https://keys.openpgp.org), der Screenshot ist etwas älter):

Adressbucheintrag in ProtonMail

1. Nach Klick auf das Zahnrad öffnet sich dieser Dialog zum Hochladen des öffentlichen Schlüssels.

Privaten Schlüssel importieren

“ Bitte lade den **privaten** Schlüssel deiner AG/WiG **nicht** auf ProtonMail hoch, sondern verwende zum Entschlüsseln von AG/WiG-E-Mails einen E-Mail-Client wie Thunderbird.

Thunderbird

“ Thunderbird muss installiert und das entsprechende Postfach eingerichtet sein.

PGP-Schlüsselpaar erzeugen

Dieser Abschnitt ist in folgenden Fällen für dich relevant:

- Du willst von deiner privaten E-Mail-Adresse verschlüsselte E-Mails verschicken.
- Du willst von deiner AG/WiG verschlüsselte Emails senden, aber ihr habt noch keinen Schlüssel.

Dazu musst du dir in Thunderbird ein Schlüsselpaar für deine E-Mail-Adresse erzeugen. Hier findest du Anleitungen dazu:

- <https://www.youtube.com/watch?v=NyOkgvVtZ10&t=101s> (ab min 1:41)
- https://www.privacy-handbuch.de/handbuch_32j.htm

Schlüssel veröffentlichen

Wenn du anderen Menschen das Hinzufügen deines Schlüssels erleichtern willst, dann lade deinen **öffentlichen** Schlüssel bei keys.openpgp.org hoch.

Dazu bei Thunderbird den öffentlichen Schlüssel exportieren und auf <https://keys.openpgp.org/upload> hochladen. Klicke auf "verifizieren" und auf den Link in der E-Mail. Wenn du einen Schlüssel für eine @letztegeneration.org-Adresse erstellt hast, dann kannst du deinen Schlüssel auch auf pgp.letztegeneration.org veröffentlichen.

Schreibe dazu eine E-Mail (am besten signiert bzw. verschlüsselt) an it-support@letztegeneration.org.

Öffentlichen Schlüssel importieren

Bevor du mit jemandem verschlüsselt kommunizieren kannst, musst du den öffentlichen Schlüssel der anderen Person in Thunderbird importieren. Wenn du beispielsweise eine verschlüsselte E-Mail an legal@letztegeneration.org schreiben möchtest, musst du erst den öffentlichen Schlüssel von legal@letztegeneration.org importieren. Du kannst das auf verschiedene Weise machen. Nützlich dabei ist das Fenster "OpenPGP-Schlüssel verwalten" in Thunderbird. Du kannst es folgendermaßen öffnen: Rechtsklick auf dein Postfach » Einstellungen » Ende-zu-Ende-Verschlüsselung » OpenPGP-Schlüssel verwalten

Hier drei Wege, wie du einen öffentlichen Schlüssel importieren kannst

- Im Fenster 'OpenPGP-Schlüssel verwalten': Schlüsselservers » Schlüssel online finden: legal@letztegeneration.org » Suchen -> auf 'Akzeptiert' klicken
- Gehe auf die Webseite pgp.letztegeneration.org » Lade die Datei 'LG_AG_Legal-678A9D067546A58E11341B7E61B9ED32301F7A23.asc' herunter » Öffne die Datei mit Thunderbird. Oder klicke auf 'Datei' » 'Öffentlichen Schlüssel aus Datei importieren' im Fenster 'OpenPGP-Schlüssel verwalten'
- Schreibe eine unverschlüsselte E-Mail an legal@letztegeneration.org und frage nach dem öffentlichen PGP-Schlüssel. Die Antwort-E-Mail enthält dann den öffentlichen Schlüssel im Anhang.

Schaut euch auch gerne [dieses Youtube-Video](#) (zweite Hälfte ist relevant) an, darin wird das auch nochmal erklärt.

Privaten Schlüssel importieren

Diese Anleitung ist für dich relevant, wenn du in einer WiG/AG mitarbeitest, die PGP-Verschlüsselung nutzt. Es wird davon ausgegangen, dass der private Schlüssel für das

entsprechende Postfach vorhanden ist.

1. Los gehts: Rechte Maustaste auf das Postfach, im Kontextmenü **Einstellungen** auswählen:



1. Links im Menü **Ende-zu-Ende-Verschlüsselung** auswählen:



1. Rechts **Schlüssel hinzufügen** auswählen:



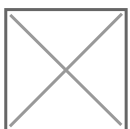
1. Dann **Bestehenden OpenPGP-Schlüssel importieren** auswählen:



1. **Datei für den Import auswählen** klicken:



1. Die Datei mit dem privaten Schlüssel auswählen:



1. Das Passwort für den Schlüssel eingeben (das muss dir jemand von der WG/AG geben):



1. Einmal **Weiter** klicken:



1. Der Import ist jetzt abgeschlossen:



1. Jetzt muss der Schlüssel noch explizit ausgewählt werden, damit er in Zukunft für verschlüsselte E-Mails verwendet wird:



1. Und als letztes ein paar Einstellungen anpassen. Zum einen **Verschlüsselung für neue Nachrichten verwenden** und **Unverschlüsselte Nachrichten digital unterschreiben**.



1.
Am besten auch weiter unten noch den Haken setzen bei "öffentlichen Schlüssel automatisch anhängen" (bzw. "Attach public key when adding an OpenPGP digital signature"). Dann kann die andere Person den öffentlichen Schlüssel gleich importieren.
2. Fertig!

Version #1

Erstellt: 5 Juli 2025 15:16:15 von RAZ Migration Bot

Zuletzt aktualisiert: 5 Juli 2025 15:16:15 von RAZ Migration Bot