# Emails verschlüsseln

Hier findest du:

- Anleitungen wie du verschlüsselte Emails einrichtest und verschickst.
- Lösungen für Webmail und lokal am Computer
- Tipps zur sicheren Verwendung
- Infos wie verschlüsselte Email-Kommunikation funktioniert

Emailverschlüsselung basiert auf sogenannter Ende-zu-Ende-Verschlüsselung. Wir haben dir in einem Artikel die grundlegende Funktionsweise von Verschlüsselungen kurz zusammengefasst.

Bei der Emailverschlüsselung reden wir von der PGP-Verschlüsselung. Die Abkürzung PGP steht dabei für eine Technologie von Verschlüsselung und bedeutet ausgeschrieben "Pretty Good Privacy". Prinzipiell legst du einen öffentlichen Schlüssel an mit dem Andere ihre Nachricht an dich verschlüsseln. Mit einem privaten Schlüssel (den nur du hast) kannst du diese Nachricht entschlüsseln. Die Erzeugung (Generierung) dieser Schlüssel übernimmt ein Programm für dich. Wie diese Schlüssel generiert werden, welche Programme du benötigst und welche Einstellungen du vornehmen musst erklären wir dir in den folgenden Anleitungen.

Die Verschlüsselung von Emailkommunikation funktioniert vereinfacht so, dass die Person, die dir eine verschlüsselte Email schicken will diese mit deinem öffentlichen Schlüssel (Public Key) verschlüsselt. Mit dem öffentlichen Schlüssel kann eine Nachricht nur verschlüsselt, nicht aber entschlüsselt werden. Für das Entschlüsseln benötigst du deinen persönlichen privaten Schlüssel (Private Key).

Der öffentliche Schlüssel ist dabei wirklich öffentlich, kann per Email verschickt werden und auch auf Schlüssel-Datenbanken ins Internet geladen werden, damit ihn auch alle finden, die dir eine verschlüsselte Email schicken wollen. Der private Schlüssel ist nur bei dir auf dem Computer und sollte niemals auf unverschlüsselten Datenträgern herumliegen oder jemand anderen gegeben werden!

Die Einrichtung der Programme und Schlüssel für die verschlüsselte Email-Kommunikation braucht etwas Zeit und Energie. Wir empfehlen dir, dich mit jemensch zusammen zu setzen, die sich bereits mit der Einrichtung von PGP-Verschlüsselung auskennt. Aber auch alleine mit entsprechenden Anleitungen ist es gut möglich, dir eine verschlüsselte Emailkommunikation einzurichten.

# Anleitungen

## Verschlüsselung lokal auf deinem Computer einrichten

## Email-Verschlüsselung mit Mozilla Thunderbird

Wir verweisen auf die hervorragene Anleitung von systemli! Dort wird neben der Einrichtung auch erklärt wie ihr eure Schlüssel austauschen bzw. bekommen könnt.

## Du benötigst das Email-Programm Thunderbird.

Das Programm Thunderbird hat im Jahr 2020 darauf umgestellt, dass verschlüsselte Emailkommunikation direkt im Programm eingebaut ist. Wenn du also die Einrichtung von Thunderbird im Internet suchst, bekommst du noch viele alte Anleitungen.

Falls wer noch eine ältere Version von Thunderbird nutzt: Vor der Programmversion Thunderbird 78.2.0 benötigte es ein sogenanntes Plugin "Enigmail" und zusätzlich unter MAC und Windows noch die Installation von weiteren Programmen. Auch macht gerade wegen dieser Umstellung bei vielen, die noch alte Versionen benutzen, die Emailverschlüsselung Probleme. Hier ist eine Anleitung wie ihr von Enigmail auf die neue Variante umstellen könnt.

So richtet ihr euer Thunderbird ein:

- 1. Installiere das Programm Thunderbird.
- 2. Richte deine bereits vorhandene Emailadresse in Thunderbird ein. Eine Anleitung für das Einrichten des Email-Programmes Thunderbird findest du bei Systemli.
- 3. Richte die Verschlüsselung ein. Eine Anleitung von Systemli für die Einrichtung der Emailverschlüsselung im Emailprogramm Thunderbird
- 4. Teste die Einrichtung zuerst aus. Schicke ein paar Emails hin und her mit jemensch, wo auch schon eine verschlüsselte Email hat. Schicke erst sensible Inhalte, wenn du dir sicher bist, dass die Verschlüsselung funktioniert und du dich ein wenig mit dem Programm vertraut gemacht hast.

#### Verschlüsselung über Webmail von Systemli

Eine einfache Methode zu einer funktionierenden Emailverschlüsselung über Webmail (also Zugriff auf deine Emails im Internetbrowser) zu kommen bietet das linke Tech-Kollektiv Systemli.

Die erste Hürde: Um bei Systemli eine Emailadresse anlegen zu können brauchst du einen Systemli Account anlegen von jemensch die bereits ein Konto bei Systemli hat. Systemli bietet diese Services unentgeltlich an - du kannst dir aber durchaus überlegen dem Kollektiv Geld zukommen zu lassen für ihren Aufwand.

Im Webmail von Systemli können bequem die Schlüssel angelegt werden und verschlüsselte Email versendet und empfangen werden. Allerdings liegen die Schlüssel dann nicht bei dir auf dem Computer, sondern bei Systemli am Server. Das ist ein Sicherheitsrisiko: Wenn sich wer Zugriff auf den Server verschaffen kann, können sich diese Personen auch deines Schlüssels bemächtigen.

Die Leute von Systemli erklären diese Problematik auch selbst auf ihrem Wiki. Dort findest du auch die Anleitung für die Verschlüsselung in deren Webmail.

## Verschlüsselt schreiben - Öffentliche Schlüssel importieren

Mit der Einrichtung des Programmes ist es leider noch nicht ganz getan.

#### o Öffentlicher Schlüssel besorgen

a) Ihr habt einen Schlüssel per Email-Anhang, per USB-Stick oder als Download bekommen: Einfach per Rechtsklick auf den Anhang (eine Datei die mit .asc endet) klicken und *Import OpenPGP Key anklicken*, dann *accepted* auswählen, anschließend auf *ok*.

b) Direkt im OpenPGP Key Manager In Thunderbird Account Settings auf End-To-End Encryption und dann den OpenPGP Key Manager anklicken. Unter Keyserver → Discover keys online könnt ihr eine Emailadresse eingeben und seht ob für diese Email-Adresse ein Schlüssel auf den Keyserver hinterlegt ist.

#### o Email verschlüsselt schreiben

Wenn du ein neues Email schreibst wähle im Feld Security die Angabe require encrytion aus.

## Anderen deinen Schlüssel geben - damit sie dir schreiben können

Damit dir andere Leute eine verschlüsselte Email schicken können benötigen sie neben deiner Emailadresse auch deinen öffentlichen Schlüssel.

#### o Öffentlichen Schlüssel per Email verschicken

Du kannst deinen Öffentlichen Schlüssel per Email verschicken:

- In Thunderbird kannst du wenn du ein Email schreibst einfach auf das Feld "Security" klicken und "Attach my Public Key" auswählen.
- Im Webmail von Systemli kannst du wenn du ein Email schreibst ebenfalls einfach "Attach my Public key auswählen.

#### o Öffentlichen Schlüssel ins Web stellen (Schlüsselserver)

Damit dich die Leute aber nicht erst fragen müssen kannst du deinen Öffentlichen Schlüssel auch auf sogenannte **Schlüsselserver im Internet** laden. Auf den Schlüssel-Server-Seiten kann dann nachgeschaut werden ob es zu deiner Email-Adresse auch einen Öffentlichen Schlüssel gibt. Zusätzlich zu den Schlüsselservern empfehlen wir dennoch deinen Öffentlichen Schlüssel einfach wie oben beschrieben an die Email anzuhängen.

Verwende am Besten den OpenPGP-Schlüsselserver auf dem du Suchen und Hochladen kannst. Das gute an diesem Schlüssel-Server ist, dass er von Thunderbird genutzt wird und hier eingetragene Schlüssel direkt in der Thunderbird-Schlüsselverwaltung gefunden werden.

- 1. Zuerst musst du einen Schlüssel exportieren.
- 2. Klicke dazu in Thunderbird rechts oben auf die drei Striche. Dann gehe auf *Tools* und dann auf *Open PGP Key Manager*. Im *Key Manager* klickst du mit der rechten Maustaste auf deine fettgedruckte Emailadresse und wählst *Export Keys to File* aus und speicher die Datei ab.
- 3. Auch im Webmail von Systemli kannst du den Öffentlichen Schlüssel exportieren. Gehe dazu auf "Setting", dann auf "PGP Keys". Klicke deinen Schlüssel bzw. deine Emailadresse an und gehe auf "Export". Achte darauf das du nur den Öffentlichen Schlüssel (Public Key) auswählst".
- 4. Gehe auf den Schlüsselserver und klicke auf upload
- 5. Wähle den zuvor exportierten Schlüssel aus und lade ihn hoch.

# Verschlüsselte Email-Verteiler

Email-Verteiler oder Email-Listen funktionieren so, dass du eine Email an die Email-Liste schreibst und diese Email dann an alle Mitglieder der Liste verschickt wird. Dabei kann Anonymität und auch Verschlüsselung gewährleistet werden.

# 🕆 Fix Me!

da etwas parat hast, melde dich gerne beim Kollektiv.

# Backup / privaten Schlüssel auf einen neues Gerät übertragen

Hier ist eine Anleitung wie ihr den privaten Key auf ein neues Gerät übertragen könnt. Auch für ein Backup macht es Sinn die Schlüssel zu exportieren und auf euer verschlüsseltes Backupmedium zu übertragen.

Wie ihr die Schlüssel exportieren und wieder importieren findet ihr in dieser Anleitung von Systemli.

# Tipps zum sicheren Umgang mit verschlüsselten Emails

Schützt euren privaten Schlüssel. Legt ihn nur auf eurem privaten Laptop ab, von dem ihr ja sicherlich die Festplatte verschlüsselt habt und macht irgendwo eine Sicherungskopie die ihr möglichst zugriffsgeschützt aufbewahrt. Verwendet eine starke Passphrase. Verwendet keine verräterischen / potenziell problematischen Betreffzeilen & verschlüsselt auch Emails, deren Inhalte nicht geheim sein müssen! Setzt euch mit FreundInnen gemeinsam zusammen und signiert gegenseitig eure Keys (das nennt sich dann Keysigining-Party).

Euer Geheimer Key ist zwar was sehr privates, jedoch ist das kein Grund einen Bund fürs Leben einzugehen. Solche Keys haben ein Ablaufdatum, das ihr beim Erstellen setzen könnt. Wählt das nicht zu weit in der Zukunft.

## Zum Weiterlesen

#### Anleitung zur Email-verschlüsselung von Systemli

Eine weitere Anleitung zu Email Verschlüsselung in der allgemein großartigen Broschüre "Beschlagnahmt" From:

https://www.fit-fuer-aktion.wiki/ - Selbstverteidigung im (anti-)politischen Alltag

Permanent link:

https://www.fit-fuer-aktion.wiki/digitale-sicherheit/sichere-kommunikation/email-verschluesseln

Last update: 2021/10/11 15:53



5/5