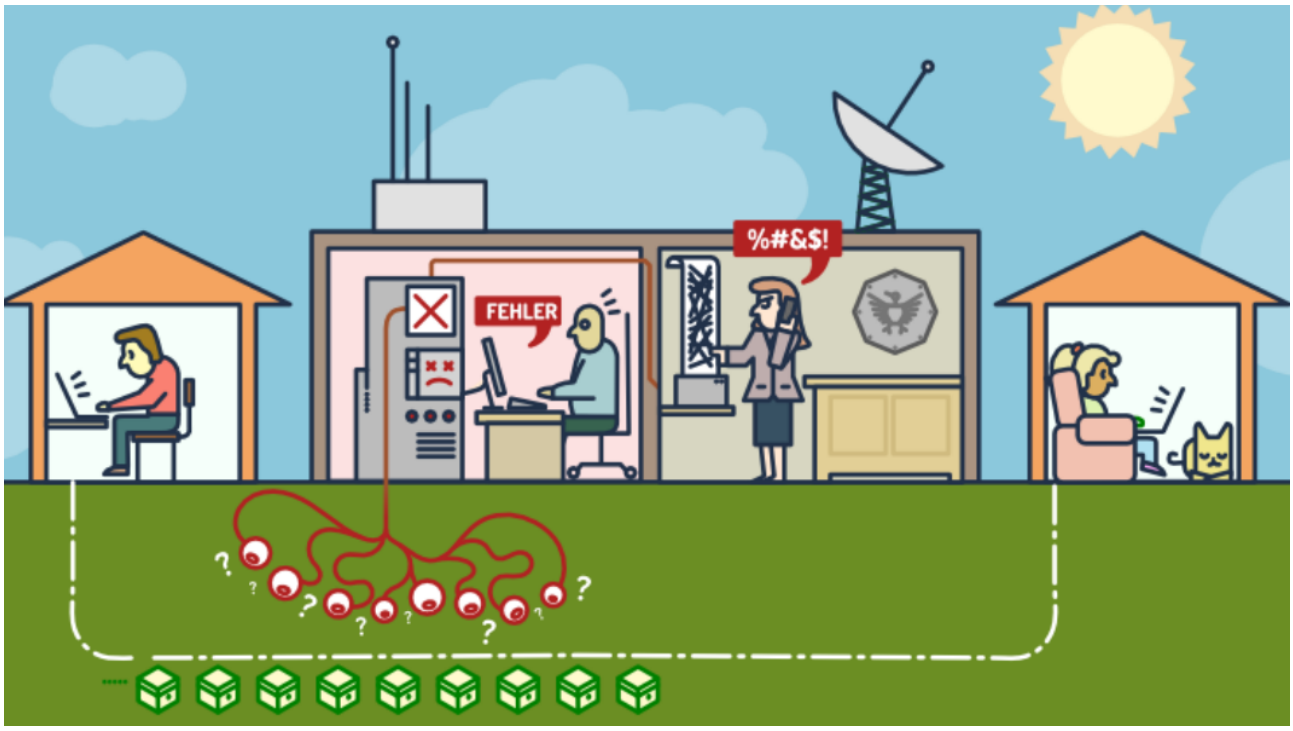
# EMAIL-SELBSTVERTEIDIGUNG

(V.2015-02)



# Inhaltsverzeichnis

# 1 Warum über E-Mail nachdenken?

E-Mailen gehört für viele Menschen zur alltäglichen Kommunikation.

Eine unverschlüsselte E-Mail ist wie eine Nachricht auf einer offenen Postkarte. Jede*r, die/der am Transport einer Postkarte oder E-Mail beteiligt ist, kann den Inhalt bei Interesse mitlesen. Wer aber alles an der Beförderung einer E-Mail beteiligt ist, bleibt für den Normalbenutzer meistens völlig undurchschaubar.

Es gibt also gute Gründe, aus der Postkarte einen verschlossenen Brief zu machen.

Die Anleitung zum „Mail verschlüsseln“ beruht zum größten Teil auf der Anleitung der Free Software Foundation und kann unter www.emailselfdefense.fsf.org/de im Netz angesehen werden. (Dort kann man auch bequem auf die Links klicken!). Einige Teile sind aus dem dem Handout der Cryptoparty des Leinelab Hannover (leinelab.de) von Michael Ebeling entnommen.

**Die Grenzen**

Selbst wenn die Inhalte verschlüsselt sein sollten, so gibt doch die Auswertung von Verbindungsdaten, also z.B. wer wann mit wem gemailt hat eine große Menge an Auskünften über Beziehungen, Verhältnisse und Netzwerke sowie die Stellung einzelner darin. Dagegen hilft die Email-verschlüsselung nicht. Um die Verbindungsdaten nicht öffentlich zu machen helfen Anonymisierungsnetzwerke wie zum Beispiel TOR.

Auch gegen Viren und ähnliche Schädlinge, die Informationen direkt am Rechner abgreifen hilft die Verschlüsselung nicht.

## 2 Email-Selbstverteidigung

Diese Anleitung bringt dir eine einfache Selbstverteidigungsmethode bei: E-Mail-Verschlüsselung. Wenn du fertig bist, kannst du E-Mails senden und empfangen, die von Überwachern oder Kriminellen, die deine E-Mails abfangen, nicht gelesen werden können. Alles was du brauchst ist ein Computer mit einer Internetverbindung, ein E-Mail-Konto und eine halbe Stunde Zeit.

Auch wenn du nichts zu verbergen hast, die Verwendung von Verschlüsselung schützt die Privatsphäre der Menschen, mit denen du kommunizierst, und macht den Systemen der Massenüberwachung die Arbeit schwer.

Sich gegen Überwachung zu wehren, erfordert neben der Verwendung von Verschlüsselung den politischen Kampf dafür, dass weniger Daten über uns gesammelt werden. Aber der erste Schritt ist es, dich selber zu schützen und die Überwachung deiner Kommunikation so schwer wie möglich zu machen.

## 3 Die Auswahl des E-Mail-Anbieters

Viele von uns arbeiten mit „kostenlosen“ E-Mail-Angeboten von Internetkonzernen wie z.B.

- web.de
- gmx.de
- yahoo.de
- googlemail.com bzw. gmail.com
- …

Leider ist das jedoch nicht wirklich „umsonst“.

Die dahinterstehenden Konzerne versuchen einerseits, mittels Kundenbindung für kostenpflichtige Zusatzdienste zu werben und erlauben sich andererseits, in den Mails ihrer Kund*innen herumzuschnüffeln. Selbstverständlich „nur“ zu Werbezwecken, aber selbst wenn das stimmen sollte, so werden damit umfangreiche Profildaten von den Benutzern gewonnen und verkauft.


Die Vergangenheit hat gezeigt, dass die kommerziellen E-Mail-Anbieter („Provider“) in aller Regel keinen großen Widerstand gegen die Herausgabe privater Daten ihrer Kunden leisten, wenn Sie von deutschen oder internationalen Behörden mit oder ohne rechtliche Grundlage dazu aufgefordert werden.

**Es gibt Alternativen zu den konzernhaften E-Mail-Anbietern**

Erste Möglichkeit: Kostenlose, politische E-Mail-Anbieter, z.B.:

- www.so36.net
- www.riseup.net
- www.nadir.org
- www.privatdemail.net

Zweite Möglichkeit: Nicht kostenlose E-Mail-Anbieter, z.B.:

- www.posteo.de (kostet 1 Euro pro Monat)
- http://jpberlin.de/ (kostet 1 Euro pro Monat)

Dritte Option:
Ihr kennt jemanden, der/die einen eigenen Server und/oder eine eigene Homepage betreibt. Im ersteren Fall könnt ihr, falls ihr der Person und seinem Serverstandort vertrauen, dort um die Einrichtung einer eigenen E-Mail-Adresse nachfragen.

Doch selbst wenn dieser Mensch nur eine eigene Homepage ohne eigenen Server betreibt, ist die Einrichtung einer E-Mail-Adresse auf dessen Homepage eventuell immer noch ein klein wenig besser/sicherer als ein E-Mail-Konto bei einem der Internet-Konzerne.

# 4 Verschlüsseln von E-Mails

Verschlüsselte E-Mails können (in aller Regel!) nur von denjenigen Menschen gelesen werden, für die diese Mail bestimmt sind. So ist es zumindest beabsichtigt.

Damit zwei Menschen miteinander verschlüsselt mailen können, müssen beide dafür vorbereitet sein. Sie müssen sich auf ein einheitliches Verschlüsselungssystem geeinigt haben und beide müssen technisch in der Lage sein, richtig damit umzugehen.

Ein gewisses Mindestmaß an Verständnis für Verschlüsselung ist notwendig. Mit der GPG- bzw. PGP-Verschlüsselung wurde ein Quasi-Standard geschaffen, der inzwischen von sehr vielen Menschen akzeptiert und verwendet wird.
Auf diese Methode möchten wir uns an dieser Stelle konzentrieren.

*So sieht eine unverschlüsselte oder wieder entschlüsselte E-Mail aus:*

```
Hallo Otto.
Wollen wir heute abend eine Portion Pommes essen gehen?
Deine Lotti.
```

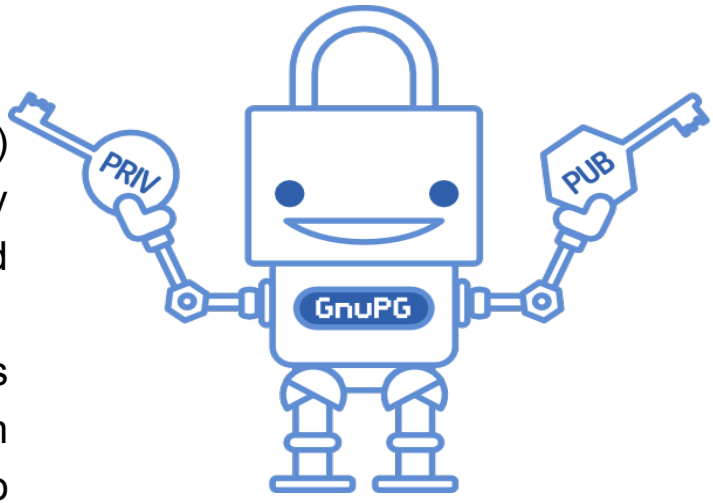
*Und das ist der gleiche Inhalt, jedoch in mittels GPG verschlüsselter Form.*

```
-----BEGIN PGP MESSAGE-----
Charset: UTF-8
Version: GnuPG v1.4.9 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEMAyjHsC5oubOFAQf6Aio0MAkA2//OH7yi8/KNyt5yRHLi209SMW6tALdZkiPB
2ZqA5lIGI9+W0Z6/IUIJVeuH7rcb8+JiflHa1QvkRA/cqx7Dx0aq8lt6KiIxR798
hLMIAplc8u3NuD2A6qB9qDlAfH6ok99sASjURavXGG2cFr/S9gB87GjgKS8pRp9R
sbtwmh5NThGCRUfOgPIsw8bBsQYrlVPe6X4f2/CBi88lVLDc01d5Wy0Ma+kjqfnX
wwCXS+qkd9BNdalvTtOeH04oPurdlPuHZsBBiPl2y3LpJ/1FKl3UqCr9rQ4/SK0Q
in01E3/1qf0P/PSwtH95EO23lPTI4nFERq2NXyXsGNKCAVdiOn/qKgBDSMO79GfG
XdtL+CgZraKsjh8cb//bHEqhRozd8kQiOPflhwTHhDGzk85+tleIXIpAyiKG1JW8
7anl7ZwP+JgxvHuMOSeqiCAS0TWkPHJcqMcY5CtuetL9FllszlFK/8m+S9QdHNAm
MWfQx/RAf0uJXAQPs42ffEGobQ==
=Y/kU
-----END PGP MESSAGE-----
```

# 5 Das Prinzip der asymmetrischen Verschlüsselung

Die Abkürzung „PGP“ steht für „Pretty Good Privacy“. Es ist ein kommerzielles Programm zur Verschlüsselung und zum Unterschreiben von Daten.




„GPG“ (oder auch: „GnuPG“) hingegen steht für „Gnu Privacy Guard“ - das ist ein freies und kostenloses Verschlüsselungsprogramm, das ebenfalls das PGP-Prinzip zum Verschlüsseln nutzt und so

gestaltet wurde, dass es eine möglichst weite Verbreitung findet.

PGP und damit GPG arbeiten mit einer so genannten asymmetrischen oder auch Public-Key-Verschlüsselung. Damit kann mit einem öffentlichen Schlüssel einen Klartext in einen Geheimtext umgewandelt werden. Daraus kann der Klartext mit einem geheimen Schlüssel wieder gewonnen werden.

Der geheime Schlüssel muss geheim gehalten werden, und es ist praktisch unmöglich, ihn aus dem öffentlichen Schlüssel zu berechnen. Der öffentliche Schlüssel muss jedem zugänglich sein, der eine verschlüsselte Nachricht an den Besitzer des geheimen Schlüssels senden will. Dabei muss sichergestellt sein, dass der öffentliche Schlüssel auch wirklich dem Empfänger zugeordnet ist

Dieses Verschlüsselungsprinzip hat sich als sicher und anwendungsfreundlich herausgestellt und wird daher sehr häufig für die Verschlüsselung von E-Mail eingesetzt.

## 6 Installiere die Programme

Diese Anleitung basiert auf der freier Software GnuPG. Bevor du GnuPG konfigurierst, brauchst du jedoch ein E-Mail-Programm.

„Thunderbird“ oder auch „Mozilla Thunderbird“ ist der Name eines kostenfreien OpenSource-Programms, mit dem man sehr einfach E-Mails lesen, schreiben und verwalten kann. Es ist für Linux, Mac OS und Windowssysteme erhältlich. Vor allem aber gibt es das komfortable Add-on Enigmail, mit dem man sehr einfach und sehr schnell mit der Verschlüsselung von E-Mails anfangen kann.

**Schritt 1: Thunderbird**
Installiere und konfiguriere dein E-Mail-Programm für dein E-Mail-Konto (wenn es nicht schon getan wurde). Öffne dazu dein E-Mail-Programm und folge dem Assistenten, der es für dein E-Mail-Konto konfiguriert.

**Schritt 2a:  Du hast ein GNU/Linux-System**
Auf den meisten GNU/Linux-Systemen ist GnuPG bereits installiert, also musst du es nicht herunterladen.

**Schritt 2b: Du hast Mac OS**
Hol dir GnuPG, indem du GPGTools herunterlädst. GPGTools ist ein Software-Paket, das GnuPG enthält. Installiere es und wähle dabei immer die vorgeschlagenen Standard-Optionen. Nachdem es installiert wurde, kannst du alle Fenster schließen, die es geöffnet hat.

**Schritt 2c: Du hast Windows**
Hol dir GnuPG, indem du GPG4Win herunterlädst
GPG4Win ist ein Software-Paket, das GnuPG enthält. Lade es herunter, installiere es und wähle dabei immer die vorgeschlagenen Standard-Optionen. Nachdem es installiert wurde, kannst du alle Fenster schließen, die es geöffnet hat.

**Schritt 3: Installiere das Enigmail-Plugin für dein E-Mail-Programm**
Klicke im Menü deines E-Mail-Programmes auf Add-ons (es könnte auch im Untermenü Extras sein). Vergewissere dich, dass auf der linken Seite Erweiterungen ausgewählt ist. Kannst du Enigmail sehen? Wenn ja, dann überspringe diesen Schritt.
Wenn nicht, suche "Enigmail" mit Hilfe der Suchleiste oben rechts. Installiere es und starte dein E-Mail-Programm anschließend neu.

# 7 Erstelle deinen Schlüssel

Um GnuPG zu verwenden, benötigt man einen öffentlichen und einen privaten Schlüssel (beide bilden ein Schlüsselpaar). Jeder Schlüssel ist eine sehr große Zahl und ist einzigartig. Beide Schlüssel sind mit einer speziellen mathematischen Funktion verbunden.

Dein öffentlicher Schlüssel ist nicht wie ein Hausschlüssel, da er im Internet auf einem Schlüsselserver gespeichert wird. Die Leute können ihn so herunterladen und ihn benutzen, wenn sie dir verschlüsselte E-Mails verschicken. Man kann sich den Schlüsselserver wie ein Telefonbuch vorstellen, von wo Leute, die dir eine Verschlüsselte E-Mail schicken möchten, deinen öffentlichen Schlüssel herunterladen können.

Dein privater Schlüssel ist eher wie ein Hausschlüssel, weil ihn niemand außer dir besitzen darf. Der private Schlüssel wird eingesetzt, wenn du E-Mails entschlüsselst.

**Erzeuge ein Schlüsselpaar**

Wähle im Menü deines E-Mail-Programmes OpenPGP → OpenPGP-Assistent. Du musst den Text im nächsten Fenster nicht unbedingt lesen, wenn du nicht willst, aber es ist eine gute Idee, die Texte der späteren Schritte des Assistenten zu lesen.
Im zweiten Schritt mit dem Titel "Unterschreiben", wähle "Nein, ich möchte in Empfängerregeln festlegen, wann unterschrieben werden soll".

Nutze die Standard-Optionen, bis du am Schritt "OpenPGP-Schlüssel erzeugen" angelangt bist.

Beim Schritt namens "OpenPGP-Schlüssel erzeugen" solltest du ein starkes Passwort verwenden! Dein Passwort sollte mindestens 12 Zeichen lang sein und mindestens je einen Kleinbuchstaben und

Großbuchstaben und mindestens eine Zahl oder ein Satzzeichen enthalten. Vergiss das Passwort nicht, sonst ist diese gesamte Arbeit umsonst!

Das Programm wird einige Minuten brauchen, um den nächsten Schritt "Schlüsselerzeugung" abzuschließen. Während du wartest, solltest du etwas anderes mit deinem Computer tun, wie einen Film anschauen oder im Web surfen. Je mehr du deinen Computer in dieser Zeit nutzt, desto schneller wird der Schlüssel generiert.

Wenn der Schritt "OpenPGP-Bestätigung" kommt, klicke auf "Zertifikat erzeugen" und speichere es an einem sicheren Ort auf deinem Computer zum Beispiel in einen Ordner namens "Widerrufszertifikat". Du solltest das Widerrufszertifikat an einen sicheren Ort kopieren -- ideal ist ein Flashmedium oder eine Festplatte, die du an einem sicheren Ort in deinem Haus aufbewahrst.

Sollte dein privater Schlüssel jemals gestohlen werden oder verloren gehen, brauchst du dieses Zertifikat, um anderen mitzuteilen, dass du dieses Schlüsselpaar nicht mehr benutzt.

**Lade deinen öffentlichen Schlüssel auf einen Schlüsselserver**
Wähle OpenPGP → „Schlüssel verwalten“... im Menü aus.
Rechtsklicke auf deinen Schlüssel und klicke dann auf „Auf Schlüssel-Server hochladen“.... Wähle dazu den voreingestellten Schlüsselserver im Pop-up.

Jetzt kann jemand, der dir eine verschlüsselte Nachricht übermitteln möchte, deinen Schlüssel vom Internet herunterladen.

## 8 Probier es aus

Wenn du gerade niemanden zum testen hast, kannst du mit einem

Programm namens Edward, dass die Free Software Foundation entwickelt hat, kommunizieren. Edward weiß, wie man E-Mails verschlüsselt. Abgesehen von den gekennzeichneten Ausnahmen sind das die gleichen Schritte, wie wenn du mit einer realen, lebenden Person kommunizierst.

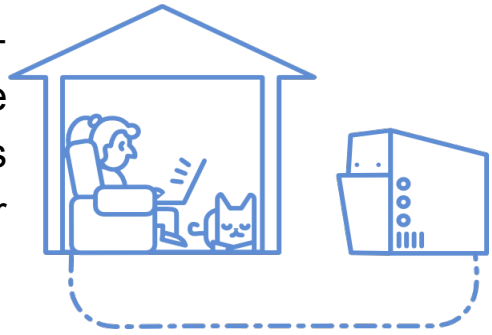
**Schick Edward deinen öffentlichen Schlüssel**

Dies ist ein spezieller Schritt, den du nicht machen musst, wenn du mit echten Menschen kommunizierst. Gehe im Menü deines E-Mail-Programms auf OpenPGP → Schlüssel verwalten. Du solltest deinen Schlüssel in der Liste sehen, die erscheint. Klicke mit der rechten Maustaste auf deinen Schlüssel und wähle dann "Öffentliche Schlüssel per E-Mail senden". Dies erstellt eine neue Nachricht, so als hättest du auf Verfassen geklickt.

Schreibe die Nachricht an edward-de@fsf.org. Schreibe mindestens ein Wort in den Betreff und in den Text der E-Mail und klicke auf Senden.
Es könnte sein, dass Edward einige Minuten braucht, um zurückzuschreiben. Ab hier tust du das gleiche, wie wenn du mit einer normalen Person kommunizierst.

**Sende eine verschlüsselte Test-E-Mail**

Schreibe eine neue E-Mail in Deinem E-Mail-Programm an edward-de@fsf.org. Schreibe "Verschlüsselungstest" oder etwas ähnliches in den Betreff und irgendetwas in den Text der Nachricht. Schicke sie noch nicht ab.



Klicke auf das Icon mit dem Schlüssel unten rechts im Fenster der E-Mail (er sollte gelb werden). Das sagt Enigmail, dass die E-Mail verschlüsselt werden soll.

Neben dem Schlüssel siehst du das Bild eines Stiftes. Das Anklicken dieses Symbols veranlasst Enigmail, eine spezielle eindeutige Unterschrift auf der Basis deines privaten Schlüssels zu deiner Nachricht hinzuzufügen.


Drücke auf Senden. Enigmail wird eine Meldung "Nicht gefundene Empfänger" zeigen.

Um eine E-Mail an Edward zu verschlüsseln benötigst du seinen öffentlichen Schlüssel. Also muss Enigmail ihn jetzt von einem Schlüsselserver herunterladen. Klicke auf "Fehlende Schlüssel herunterladen", wähle den ersten (Schlüssel-ID C09A61E8) und klicke dann auf OK. Klicke im nächsten Pop-up-Fenster wieder auf OK.
Jetzt bist du zurück beim Dialog "Nicht gefundene Empfänger". Wähle Edwards Schlüssel aus der Liste aus und klicke OK. Sollte die E-Mail nicht automatisch versendet werden, kannst du jetzt auf Senden drücken.

**Der Betreff wird nicht verschlüsselt**

Auch wenn du die E-Mail verschlüsselst, bleibt der Betreff unverschlüsselt, also solltest du dort keine vertraulichen Informationen hineinschreiben. Die Sender- und Empfängeradressen werden ebenfalls nicht verschlüsselt und können deshalb von einem Überwachungs-system gelesen werden. Wenn du Anhänge versendest, wird Enigmail dir anbieten, sie zu verschlüsseln.
Es ist sinnvoll, das Schlüsselsymbol in deiner E-Mail anzuklicken, **bevor** du anfängst zu schreiben. Ansonsten könnte dein E-Mail-Programm einen unverschlüsselten Entwurf auf dem E-Mail-Server speichern, der dort ausspioniert werden könnte.

**Empfange eine Antwort**

Wenn Edward deine E-Mail empfangen hat, entschlüsselt er sie mit

seinem privaten Schlüssel. Dann wird er deinen öffentlichen Schlüssel von einem Schlüsselserver holen und ihn verwenden, um die Antwort an dich zu verschlüsseln.

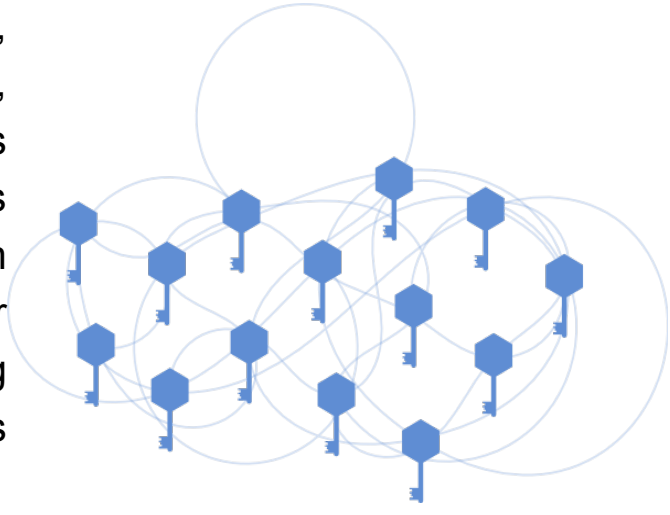
Da du die E-Mail mit Edwards öffentlichem Schlüssel verschlüsselt hast, braucht man Edwards privaten Schlüssel, um die E-Mail entschlüsseln zu können. Nur Edward besitzt seinen privaten Schlüssel, also kann niemand außer ihm — nicht einmal du — die E-Mail entschlüsseln.
Edward braucht vermutlich zwei, drei Minuten, um zu antworten.

Wenn du Edwards E-Mail bekommst und sie öffnest, erkennt Enigmail automatisch, dass sie mit deinem öffentlichen Schlüssel verschlüsselt wurde, und wird dann deinen privaten Schlüssel benutzen, um sie zu entschlüsseln.

Beachte die Leiste mit Informationen über Edwards Schlüssel, die über der Nachricht eingeblendet wird.

## 9 Das Web-of-Trust

E-Mail-Verschlüsselung ist zwar eine leistungsfähige Technologie, sie hat aber eine Schwäche: Sie benötigt eine Methode zur Überprüfung, ob ein öffentlicher Schlüssel tatsächlich der angegebenen Person gehört. Ansonsten gäbe es keine Möglichkeit, eine Angreiferin davon abzuhalten, Schlüssel mit dem Namen deines Freundes zu erstellen und sich als dein Freund auszugeben. Aus diesem Grund haben die Programmierer freier Software, die E-Mail-Verschlüsselung erfunden haben, Signaturen und das Web of Trust erfunden.



Wenn du den Schlüssel von jemandem signierst, dann sagst du öffentlich, dass du glaubst, dass der Schlüssel tatsächlich dieser Person gehört und nicht einem Betrüger. Leute, die deinen öffentlichen Schlüssel benutzen, können sehen, wie viele Signaturen er erhalten hat. Wenn du GnuPG einige Jahre lang verwendet hast, kannst du hunderte Signaturen haben. Das Web of Trust ist eine Konstellation aller GnuPG-Nutzer, die durch Signaturenketten zu einem riesigen Netz verbunden sind. Je mehr Signaturen ein Schlüssel hat und je mehr Signaturen die Schlüssel derjenigen, die unterschrieben haben, erhalten haben, desto vertrauenswürdiger ist dieser Schlüssel.

Gleichzeitig lassen sich allerdings auch Netzwerke nachvollziehen, da ja öffentlich einsehbar ist, wer den Schlüssel signiert hat.

Öffentliche Schlüssel werden normalerweise anhand ihres Fingerabdrucks identifiziert, einer Zeichenkette wie F357AA1A5B1FA42CFD9FE52A9FF2194CC09A61E8 (für Edwards Schlüssel). Sehen kannst du den Fingerabdruck deines öffentlichen Schlüssels – und anderer öffentlicher Schlüssel, die du gespeichert hast, indem du zu Enigmail → Schlüssel verwalten im Menü deines E-Mail-Programms gehst und dann mit der rechten Maustaste auf den Schlüssel klickst und die Schlüsseleigenschaften auswählst. Es ist sinnvoll, deinen Fingerabdruck immer weiterzugeben, wenn du anderen deine E-Mail-Adresse mitteilst, so dass diese Menschen kontrollieren können, ob sie deinen richtigen Schlüssel von einem Schlüsselserver herunterladen.

Du wirst sehen, dass man sich auch über die Schlüssel-ID auf öffentliche Schlüssel bezieht, dabei handelt es sich einfach um die letzten 8 Zeichen des Fingerabdrucks, z.B. C09A61E8 für Edward. Die Schlüssel-ID ist direkt im Fenster Schlüssel verwalten sichtbar. Diese

Schlüssel-ID ist wie der Vorname einer Person (es ist eine nützliche Abkürzung, aber ist vielleicht nicht eindeutig), während der Fingerabdruck tatsächlich den Schlüssel eindeutig und ohne Möglichkeit der Verwechslung identifiziert.

### 10 Schlüssel signieren

Bevor du einen Schlüssel einer realen Person signierst, überprüfe stets, ob der Schlüssel ihr gehört und ob sie ist, wer sie behauptet zu sein. Frage sie nach ihrem Ausweis (außer du vertraust ihr sehr stark) und dem Fingerabdruck ihres öffentlichen Schlüssels -- nicht nur nach der kurzen Schlüssel-ID, die zusätzlich auch zu einem anderen Schlüssel gehören könnte. Antworte ehrlich auf die Frage "Haben Sie überprüft, ob dieser Schlüssel tatsächlich dem oben genannten Absender gehört?" in Enigmail..
Gehe in deinem E-Mail-Programm zu Enigmail → Schlüssel verwalten.
Klicke mit der rechten Maustaste auf Edwards öffentlichen Schlüssel und wähle "Unterschreiben" aus dem Kontextmenü aus.
Im Pop-up-Fenster wähle "Keine Antwort" und klicke auf OK.
Zurück in Enigmail-Schlüssel verwalten wähle Schlüssel-Server → Schlüssel hochladen und klicke auf OK.

## 11 GnuPG richtig verwenden

Alle nutzen GnuPG ein wenig anders, aber es ist wichtig, ein paar wesentliche Regeln zu befolgen, um deine E-Mails zu sichern. Wenn du sie nicht befolgst, gefährdest du die Privatheit der Menschen, mit denen du kommunizierst, und deine eigene, und du beschädigst das Web of Trust.

### Wann soll ich verschlüsseln?

Je öfter du deine Nachrichten verschlüsselst, desto besser. Wenn du E-Mails nur hin und wieder verschlüsselt, könnte jede verschlüsselte Nachricht die Aufmerksamkeit der Überwachungssysteme wecken.

Wenn alle oder die meisten deiner E-Mails verschlüsselt sind, wissen die Überwacher nicht, wo sie anfangen sollen.
Das heißt nicht, dass es sinnlos ist, nur einige Nachrichten zu verschlüsseln -- es ist ein guter Start und macht Massenüberwachung schwieriger.

**Nimm dich vor ungültigen Schlüsseln in acht**

GnuPG macht E-Mails sicherer, aber es ist immer noch wichtig, nach ungültigen Schlüsseln Ausschau zu halten, die in die falschen Hände gefallen sein könnten. E-Mails, die mit ungültigen Schlüsseln verschlüsselt worden sind, könnten von Überwachungsprogrammen gelesen werden.


Gehe in deinem E-Mail-Programm zurück zur zweiten E-Mail, die dir Edward gesendet hat. Weil sie mit deinem Schlüssel verschlüsselt wurde, gibt es oben eine Leiste, die sagt, dass die E-Mail verschlüsselt ist. Wenn Du GnuPG benutzt, gewöhne es dir an, dass du auf diese Leiste schaust. Enigmail wird dich dort warnen, wenn Du eine E-Mail erhältst, die mit einem nicht vertrauenswürdigen Schlüssel verschlüsselt worden sind.

**Speichere dein Widerrufszertifikat an einem sicheren Ort**

Erinnerst du dich daran, als du deine Schlüssel erzeugt hast und das Widerrufszertifikat gespeichert hast, das GnuPG erzeugt hat? Nun solltest du das Zertifikat wirklich an einen sicheren Ort zu kopieren!!

Sollte dein privater Schlüssel jemals gestohlen werden oder verloren

gehen, brauchst du dieses Zertifikat, um anderen mitzuteilen, dass du dieses Schlüsselpaar nicht mehr benutzt.

**Reagiere schnell, wenn jemand deinen privaten Schlüssel bekommt**

Wenn du deinen privaten Schlüssel verlierst oder ihn jemand anders erhält (z.B. wenn jemand deinen Computer stiehlt oder sich unberechtigt Zugang verschafft), ist es wichtig, ihn sofort zurückzuziehen, bevor ihn jemand benutzt, um deine verschlüsselten E-Mails zu lesen. Wie dies geht, wird in dieser Anleitung nicht beschrieben, du kannst dies aber im Handbuch von GnuPG nachlesen. Wenn du mit dem Widerruf fertig bist, schicke eine E-Mail an alle, mit denen du normalerweise deinen Schlüssel benutzt, um sie zu informieren.

**Mache deinen öffentlichen Schlüssel zu einem Teil deiner Online-Identität**

Füge als erstes deinen Schlüssel-Fingerabdruck zu deiner E-Mail-Signatur hinzu. Dann schreibe an mindestens fünf deiner Freunde eine E-Mail, um ihnen mitzuteilen, dass du gerade GnuPG eingerichtet hast, und um den Fingerabdruck deines öffentlichen Schlüssels bekanntzugeben.

## 12 Alternative zum E-Mailen: Jabber

Doch muss es immer gleich eine E-Mail sein?
Insbesondere bei vielen jüngeren Leuten geht der Trend weg vom Mailen und hin zum Chatten bzw. „Short- oder Instant-Messaging“.

Von der Verwendung der Facebook-, ICQ- oder Microsoft-Messenger-Standards raten wir dringend ab. Aber es gibt eine gute Alternative dazu:

**Das so genannte „Jabbern“**

Unter „Jabber“ versteht man einen „Instant-Messaging-Standard“ namens „XMPP“.



Hört sich schlimm an, ist aber ganz einfach.

Mit dem ebenfalls freien und kostenlosen OpenSource-Programms mit dem Namen **„Pidgin“** kann sich jedermensch eine eigene Pidign-Identität erzeugen, mit deren Hilfe er/sie verschlüsselt chatten bzw. „Instant Messaging“ betreiben kann.
Das dabei zur Verschlüsselung eingesetzte System (bzw. „Protokoll“) nennt sich „OTR“ (abgekürzt für: Off-the-record Messaging).

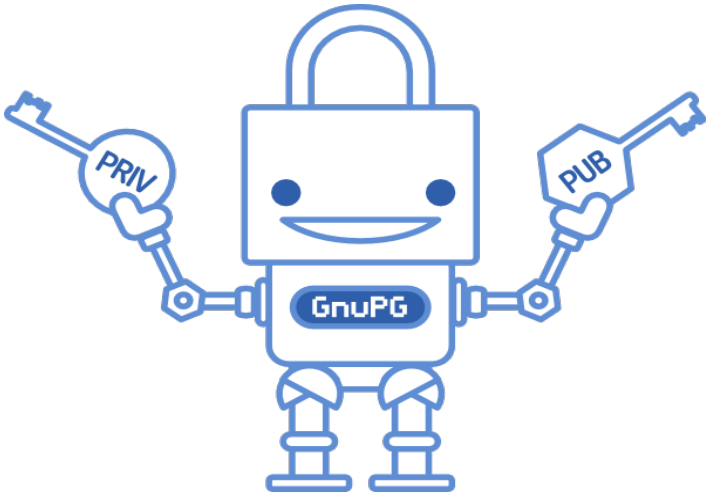
Jabber erlaubt eine schnelle und unkomplizierte verschlüsselte Unterhaltung zwischen zwei oder mehreren Menschen. Viele Verabredungen und Diskussionen lassen sich mit Jabber bzw. Pidgin sehr viel einfacher und effektiver gestalten als per Mail oder per Telefon.

## 13 Lizenz und Bildquellen



Dies Booklet ist ein Remix von fmaier aus dem Handout der Cryptoparty des Leinelab Hannover (leinelab.de) von Michael Ebeling, und der sehr empfehlenswerten Webseite der Free Software Foundation zu Emailselbstverteidigung: https://emailselfdefense.fsf.org/de

**Bilderquellen:**
Die meisten Graphiken sind von https://emailselfdefense.fsf.org/de, CC
Seite 5: Orginal von http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html nach einer Idee von http://i.imgur.com/WiOMq.jpg, Übersetzung und deutsche Variante von http://www.devianzen.de, Deutsche Übersetzung von http://devianzen.de


PRIV
PUB
GnuPG