GPG Verschlüsselung

E-Mails sicher versenden

Inhaltsverzeichnis

Allgemeines

Die Versendung einer E-Mail ist in der digitalen Welt so, als ob man eine Postkarte aus dem Urlaub schickt. Jeder Internetnutzer, der die Datenströme lesen kann, kann auch diese Postkarte lesen. Auch dein Nachbar ist theoretisch dazu in der Lage. Die bösen Buben im Internet und die Geheimdienste können das allemal.

Dem muss ein Riegel vorgeschoben werden. Abhilfe schafft hier die Verschlüsselung der E-Mails. Lesen soll deine E-Mail nur derjenige, an den die E-Mail gerichtet ist. Wohlgemerkt, der Empfänger der E-Mail muss sich ebenfalls mit der Verschlüsselung auseinandersetzen.

Die Einrichtung der Verschlüsselung gar nicht so schwer.

Da es diverse grafische Tools bei den verschiedenen Linux-Distributionen gibt, erstelle ich hier eine für alle Linux-Versionen geeignete Beschreibung.

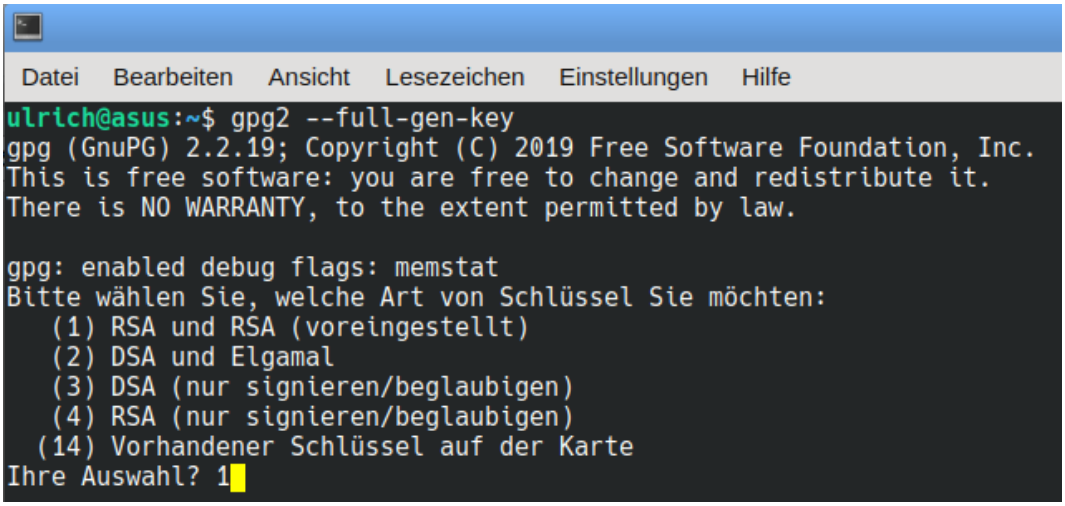
Erforderliche Programme

Die nötigen Programme sind in den Paketquellen jeder Linux-Distribution enthalten. Die Installation erfolgt einfach über die Paketverwaltung oder in der Konsole/im Terminal mit der Befehlsfolge „sudo apt install [programmname]“. Die Programme sind:

- gnupg
- gnupg2
- gpg
- gpg-agent

Die Programme können in einem Rutsch mit dem Aufruf „sudo apt install gnupg gnupg2 gpg-agent gpa“ installiert werden.

Einrichtung beginnen



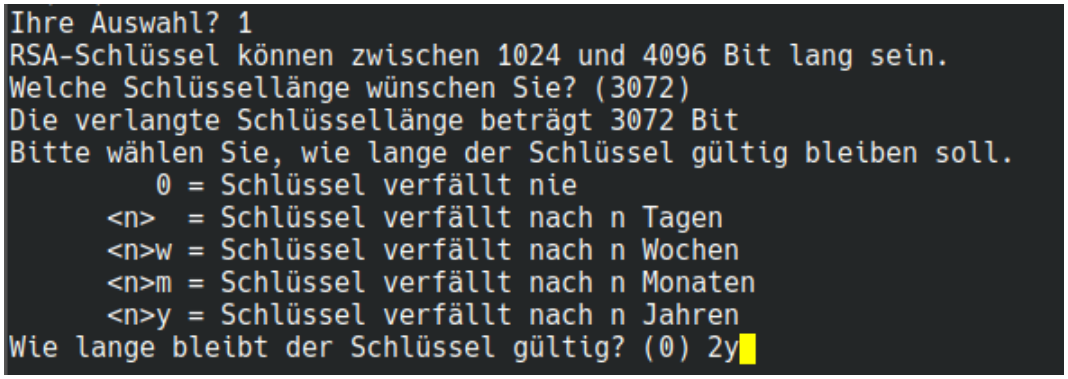
Allen Linux-Distributionen gemeinsam ist die Ersteinrichtung über die Konsole/das Terminal mit dem Aufruf „gpg2 --full-gen-key“.

Von hier an gilt es alle weiteren Einträge mit großer Sorgfalt zu erledigen. Zusätzlich sollte man Papier und Stift bereithalten, um wichtige Daten zu notieren und aufzubewahren.

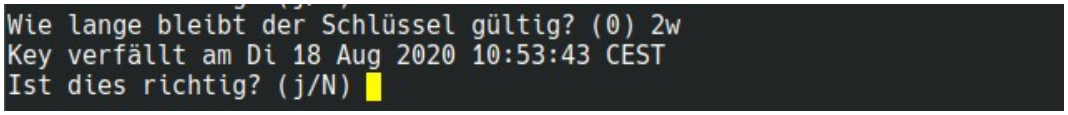
Die Voreinstellungen bleiben so wie sie dargestellt sind. In das Feld „Ihre Auswahl“ wird eine „1“ gesetzt.

Schlüssellänge und Gültigkeitsdauer

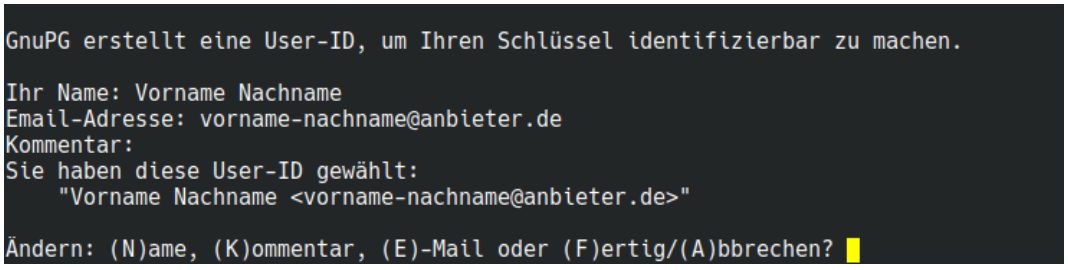
In der folgenden Abfrage kann die Länge des Schlüssels bestimmt werden. Hier gilt, je größer die Schlüssellänge ist, umso sicherer ist die Verschlüsselung. Der Wert von 3027 kann verwendet werden, 4096 Bit ist letztendlich die bessere Wahl. Je nach Ausstattung der PC-Hardware kann die Erstellung des Schlüssels einige Zeit in Anspruch nehmen.



Die Frage nach der Dauer der Gültigkeit des Schlüssels mag jeder Nutzer für sich selber entscheiden. Verfällt der Schlüssel nie, braucht man sich um Nichts weiter zu kümmern. Wird ein Verfallsdatum angegeben, muss man sich um diesen Zeitpunkt wieder neue Gedanken zur Schlüsselverwendung machen. Das Verfallsdatum kann später aber auch geändert/verlängert werden. In diesem Beispiel soll der Schlüssel für 2 Jahre gültig sein.



Nachfolgend werden der Name, die E-Mail-Adresse und ein Kommentar abgefragt.



Ihr Name	Hier sollte der echte Name eingetragen werden.
Email-Adresse:	Die Email-Adresse, für die der Schlüssel gültig ist.
Kommentar:	Kann ausgefüllt werden. Eingabe nicht zwingend erforderlich. Der Kommentar wird neben dem Namen/E-Mail-Adresse in den grafischen Tools mit angezeigt.

Danach besteht noch einmal die Möglichkeit die Eingaben zu prüfen und evtl. noch zu ändern.

Sind alle Daten korrekt, wird mit der Eingabe „(F)ertig“ die Erstellung des Schlüssels begonnen. Hier wird dann noch die Passphrase abgefragt. Bei der Eingabe ist größte Sorgfalt geboten. Ist dies doch der Eintrag, mit dem eine spätere Bearbeitung erst möglich ist.

Passphrase, was ist das

Die Passphrase kann man mit einem absolut geheimen Passwort vergleichen. Wird die Passphrase vergessen oder kommt abhanden, kann zukünftig der Schlüssel nicht mehr bearbeitet werden.

Es ist unabdingbar, dass die Passphrase an sicherer Stelle, auch in einem geeigneten Passwortmanager gespeichert wird. Keinesfalls darf die Passphrase im Internet gespeichert werden.

```
Ändern: (N)ame, (K)ommentar, (E)-Mail oder (F)ertig/(A)bbrechen? f
Wir müssen eine ganze Menge Zufallswerte erzeugen.  Sie können dies
unterstützen, indem Sie z.B. in einem anderen Fenster/Konsole irgendetwas
tippen, die Maus verwenden oder irgendwelche anderen Programme benutzen.
Wir müssen eine ganze Menge Zufallswerte erzeugen.  Sie können dies
unterstützen, indem Sie z.B. in einem anderen Fenster/Konsole irgendetwas
tippen, die Maus verwenden oder irgendwelche anderen Programme benutzen.
gpg: Schlüssel AF63C4DA30721E70 ist als ultimativ vertrauenswürdig gekennzeichnet
gpg: Widerrufzertifikat wurde als '/home/ulrich/.gnupg/openpgp-revocs.d/6875F36B1B6D91701
ACDEC54AF63C4DA30721E70.rev' gespeichert.
Öffentlichen und geheimen Schlüssel erzeugt und signiert.

gpg: keydb: handles=2 locks=1 parse=1 get=1
gpg:        build=1 update=0 insert=1 delete=0
gpg:        reset=3 found=1 not=1 cache=0 not=1
gpg: kid_not_found_cache: count=0 peak=1 flushes=1
gpg: sig_cache: total=4 cached=0 good=0 bad=0
gpg: random usage: poolsize=600 mixed=11 polls=0/28 added=168/6720
              outmix=0 getlvl1=0/0 getlvl2=0/0
gpg: rndjent stat: collector=0x0000000000000000 calls=0 bytes=0
gpg: secmem usage: 1344/65536 bytes in 2 blocks
pub   rsa3072 2020-08-06 [SC] [verfällt: 2020-08-08]
      6875F36B1B6D91701ACDEC54AF63C4DA30721E70
uid                      Vorname Nachname <vorname-nachname@anbieter.de>
sub   rsa3072 2020-08-06 [E] [verfällt: 2020-08-08]

ulrich@asus:~$
```

Damit ist die Erstellung eines Schlüssels für den sicheren E-Mail-Verkehr fertig. Die Signierung des Schlüssels ist damit auch erfolgt.

Verwendung im E-Mail-Programm

Es gibt eine Vielzahl von E-Mail-Programmen. Eine Beschreibung für einzelne Programme ist deshalb nicht möglich. In der Regel erkennen die Mailprogramme, dass eine Verschlüsselung eingerichtet worden ist. In den meisten Programmen lässt sich dies aber in den Einstellungen auch nachsehen.

Probleme mit Thunderbird

Nutzer von Thunderbird bis Version 68 müssen zusätzlich noch das „enigmail-Plugin“ als Add-On installieren oder „enigmail“ aus den Quellen nachinstallieren. Ab Thunderbird 78.2.1 ist „enigmail“ nicht mehr erforderlich, auch nicht installierbar. Es werden die allgemeinen GnuPG Programme verwendet. Im Februar 2020 wies Thunderbird noch Fehler auf. Die Betreff-Zeile wird verschlüsselt, obwohl dies nicht GnuPG konform ist. Beim anderen E-Mail-Empfänger wird der Betreff nicht korrekt angezeigt.

Ab der Version 78.2.1 verwendet Thunderbird zwar GnuPG. Alle Einstellungen dazu werden aber im Thunderbird-Profilverzeichnis gespeichert. Die nach dem hier beschriebenen Verfahren erstellten Schlüssel können aber importiert werden. Nachbearbeitungen können Probleme bereiten, da die Verzeichnisse von GnuPG und das Thunderbird-Profilverzeichnis nicht abgeglichen werden.

Was muss der Empfänger tun

Der Empfänger von verschlüsselten Nachrichten muss die hier beschriebenen Schritte ebenfalls durchführen. Die Verschlüsselung funktioniert nur, wenn Sender und Empfänger die Verschlüsselung eingerichtet haben.

Öffentlicher und privater Schlüssel

Der Verschlüsselungsschlüssel besteht aus einem öffentlichen Schlüssel und einem privaten Schlüssel. Der private Schlüssel verbleibt immer beim Ersteller der Verschlüsselung. Der öffentliche Schlüssel muss dagegen dem Empfänger von E-Mails bekannt gegeben werden.

Der öffentliche Schlüssel kann deshalb erstmalig mit einer nicht verschlüsselten E-Mail mitgesendet werden.

Verfahren

- Dem Empfänger von Verschlüsselungsmails muss der öffentliche Schlüssel bekannt gegeben werden. Das geschieht erstmals mit einer unverschlüsselten Nachricht, an die der öffentliche Schlüssel angehängt wird.
- Der Empfänger muss den so mitgeteilten Schlüssel mit seinem Schlüsselmanager importieren.
- Erst dann besteht die Möglichkeit verschlüsselte Nachrichten untereinander auszutauschen.

Grafische Tools / Schlüsselmanager

Die Distributionen verwenden für die Bearbeitung der Verschlüsselungsdaten unterschiedliche grafische Tools oder Schlüsselverwaltungsprogramme. Hier ist die Aktivität des Nutzers gefordert.

Zu den Tools gehören z. B.:

- enigmail (Thunderbird Plugin) ab Thunderbird 78.* nicht mehr erforderlich
- gpa
- kgpg
- kleopatra

Eventuell muss das Schlüsselverwaltungsprogramm nach der Erstellung der Schlüssel einmal neu gestartet werden.

Ganz wichtig

Die Schlüssel dürfen auf dem eigenen Rechner nicht gelöscht werden. Wird der Schlüssel dennoch gelöscht, sind die E-Mails je nach Einstellung im E-Mail-Programm unwiederbringlich verloren.

Übernahme der Schlüsseldaten auf einen anderen PC

Möchte man die Verschlüsselung von E-Mails auch auf einem anderen PC einsetzen gibt es ein ganz einfaches Verfahren.

PC auf dem die Daten vorhanden sind

Die Schlüsseldaten werden im versteckten Ordner „.gnupg“ im eigenen Home-Verzeichnis gespeichert. Diesen Ordner braucht man nur auf einen USB-Stick zu kopieren.

Auf dem neuen PC

Sollte auf dem neuen PC der versteckte Ordner „.gnupg“ schon vorhanden sein, ist dieser samt Inhalt zu löschen. Vom USB-Stick ist nun der gesamte Ordner .gnupg auf den anderen PC in den eigenen Home-Ordner zu kopieren. Spätestens nach einem Neustart stehen jetzt auch alle Schlüssel zur Verfügung.

Was nicht beschrieben ist

Die nachfolgenden Punkte sind für die Verwendung der Verschlüsselung nicht zwingend erforderlich. Eine Beschreibung erfolgt deshalb hier nicht.

- Weiterführenden Einstellungen am Beginn der Verschlüsselung
- Veröffentlichung der Schlüssel auf Schlüsselservern im Internet
- Verwendung von Widerrufsschlüsseln (nur bei Veröffentlichung im Internet erforderlich)
- Sicherung und Wiederherstellung der Schlüssel
- Beglaubigungen
- Zusätzliche Adressen hinzufügen

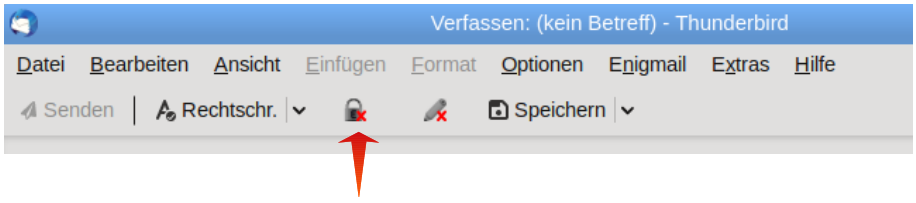
Weitere Informationen

Erste Anlaufstelle für weitere und weiterführende Informationen ist:

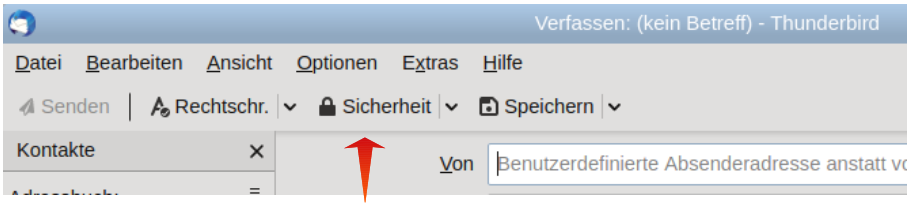
- https://wiki.ubuntuusers.de/GnuPG/

Beispiel – Anzeige der Buttons für die Verschlüsselung

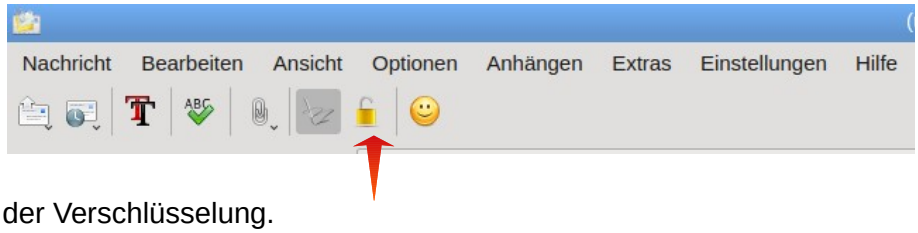
Bis Thunderbird 68.*:



Ab Thunderbird 78.*:



In Kmail:



Button zum Ein/Ausschalten der Verschlüsselung.

Geht das auch mit Windows oder Mac Computern

Nach dem Download der erforderlichen Dateien (Recherche im Internet erforderlich) kann die Verschlüsselung wie hier beschrieben im entsprechenden Terminal / Eingabeaufforderung durchgeführt werden.

Download für Windows: https://gnupg.org/index.html