Mit KMail verschlüsselte E-Mails verschicken...

Dieses Tutorial beschreibt, wie man mit dem KDE-E-Mailprogramm KMail unter Linux ganz einfach Mails signiert, verschlüsselt und entschlüsselt. Es richtet sich an Neulinge, die sicher kommunizieren wollen, daher geht es in manchen Punkten in die Tiefe der Materie.

Version vom 22. November 2002
Aktuelle Versionen unter: http://linux.waluga.de

Inhalt :

Vorwort

Wozu soll ich denn Mails verschlüsseln oder signieren – da geht doch nur Zeit drauf!
Das habe ich mir auch mal gedacht, doch als ich mich mit dem Thema genauer befasst habe, wandelte sich dieses Vorurteil schnell! Denn KMail in Verbindung mit GnuPG (oder OpenPGP) ist ein ideales Werkzeug um wirklich sicher und vertrauensvoll miteinander zu kommunizieren.
Viele Faktoren sprechen für eine Verschlüsselung oder zumindest eine Signatur von E-Mails:

- Daten werden sicher und unverfälscht übermittelt
- man hat 100%ige Gewissheit, dass keiner mitliest
- keiner kann spionieren -> kein „gläserner Mensch“ mehr
- die Mail kann nur von der Person, die man erreichen will, gelesen werden

Diese und andere Vorteile haben mich überzeugt, sodass ich nun meine Mails zumindest signiere, damit mein Gegenüber weiß, dass meine Mail auch nicht von einem Dritten gelesen bzw. verändert wurde. Für brisante und private Mails verwende ich die sehr gute Verschlüsselung.
Ich hoffe, dass auch Sie durch diese Anleitung lernen, Ihre Mails vor ungewollten Blicken zu schützen. Es ist jedenfalls einfacher und komfortabler, als Sie denken.

---

1. Was brauche ich?

1.1 GnuPG installieren

Ganz klar: Man braucht die Software, die Ihre Daten verschlüsseln kann. Als OpenSource-Anhänger verwenden wir nun eine frei zugängliche Software, die, entgegen der Meinung von OpenSource-Gegnern, extrem sicher ist – man kann sogar sagen, dass der verwendete mathematische Algorithmus unknackbar ist. Leistungsstarke Super-Computer bräuchten tausende Jahre, um den Code zu knacken, sollte man das Passwort nicht haben.

Die Software bekommt man kostenlos auf der offiziellen Seite:

http://www.gnupg.org oder direkt unter http://www.gnupg.org/download.html

Nachdem Sie das Quelltextpaket heruntergeladen haben, müssen Sie es entpacken und als Programm übersetzen.
Gehen Sie hierzu in die Konsole und in das Verzeichnis, in dem das Paket liegt. Entpacken Sie es mit dem Befehl

tar -xvzf gnupg-x.y.z.tar.gz

anschließend geben Sie nacheinander folgende Befehle ein, damit Sie eine ausführbare Datei erzeugen und das Programm systemweit zur Verfügung stellen

```
./configure
make
su [Passwort eingeben]
make install
exit
```

Anmerkung: Es ist empfehlenswert GPG 1.0.7 oder höher zu verwenden, da es beim Versionswechsel von GPG 1.0.6 zu Problemen mit den signierten Schlüsseln kommen kann; das Problem lässt sich mit Hilfe von http://linux.waluga.de/tipps/tipps.htm beheben.

1.2 Kgpg installieren

Die eben installierte Software ist für den täglichen Einsatz ungeeignet, da sie komplett von der Konsole aus bedient werden muss. Das KDE-Programm Kgpg setzt genau da an und stellt Ihnen eine grafische Oberfläche zur Verfügung, mit der Sie die grundlegenden Sachen komfortabel erledigen können.
Auch dieses Programm müssen Sie von

http://devel-home.kde.org/~kgpg/index.html

herunterladen und anschließend kompilieren. Folgende Schritte sind durchzuführen (für eine ausführliche Erklärung vergleiche mit 1.1):

```
tar -xvzf kgpg-x.y.z.tar.gz
./configure   (evtl. mit „--prefix=$KDEDIR“ oder direkt „--prefix=/opt/kde3“ bei einer
               Standardinstallation von SuSE 8.x)
make
su [Passwort eingeben]
make install
exit
```

So, Herzlichen Glückwunsch, Sie haben nun alle benötigten Programme auf Ihrem Computer eingrichtet.

1.3 GnuPG von SuSE-CD installieren

Noch einfacher können Sie beide benötigten Programme installieren, wenn Sie Ihre SuSE 8.x CDs oder die DVD zur Hand nehmen. Starten Sie YaST, dann weiter zum Modul Software / Software installieren. Klicken Sie auf „Suche“ und geben Sie „gpg“ ein. Markieren Sie das Paket mit der Beschreibung „GNU Privacy Guard, Ver/Entschlüsselungssoftware“, um diese später zu installieren.
Nun klicken Sie auf „OK“ und werden nun aufgefordert, die entsprechenden CDs einzulegen. Folgen Sie den Anweisungen... und schon haben Sie die benötigten Pakete installiert.

2. Umgang mit Kgpg

Hier wird beschrieben, wie Sie mit dem GPG-Frontend „Kgpg“ für KDE umgehen. Es werden die wichtigen Dinge angesprochen, die Sie beherrschen sollten. Es soll Sie aber nicht davon abhalten mit dem Programm ein wenig „rumzuspielen“!

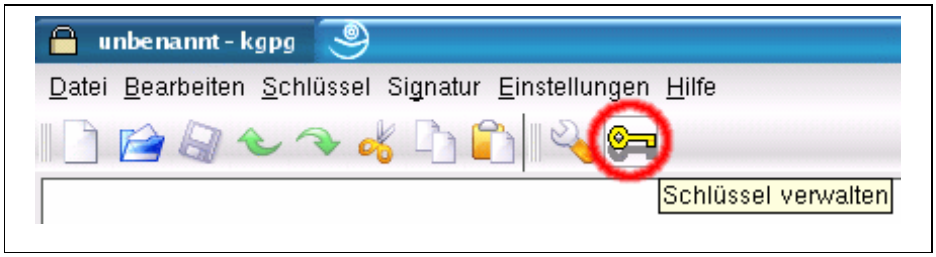
So sieht Kgpg mit seinen Schlüsselverwaltungsfunktionen aus

2.1 eigenen Schlüssel erzeugen

Um überhaupt Ihre E-Mails signieren oder verschlüsseln zu können, benötigen Sie einen eigenen Schlüssel, der, wie der Name schon sagt, nur Ihnen gehört. Dieser Schlüssel ist einmalig und eindeutig identifizierbar. Dieser besteht aus zwei Teilen:

- ein öffentlicher Schlüssel: diesen sollten Sie so öffentlich wie möglich machen, wie z.B. diesen immer an Ihre E-Mails anhängen, auf Ihrer Homepage zum Download anbieten oder ihn auf einem sogenannten Keyserver anbieten. Wie Sie das machen, entnehmen Sie bitte der sehr guten Anleitung, die Sie unter http://www.sicherheit-im-internet.de abrufen können. Denn nur wenn jemand Ihren öffentlichen Schlüssel hat, kann er Ihnen eine verschlüsselte E-Mail schicken oder die Echtheit Ihrer signierten Mail überprüfen. Wieso das so ist, wird später erklärt.
- ein privater Schlüssel: diesen dürfen Sie auf keinen Fall (!) weitergeben, denn es ist IHR Schlüssel. Mit diesem Schlüssel entschlüsseln Sie die E-Mails, die Ihnen von den anderen Personen zugeschickt werden. Außerdem wird der private Schlüssel dazu benutzt, E-Mails zu verschlüsseln und zu signieren. Sie können diesen gerne auf eine Diskette sichern, aber nur, wenn sie sicher aufbewahrt wird. Näheres dazu gleich.

Nach heutigen Erkenntnissen kann aus einem öffentlichen Schlüssel kein privater Schlüssel erzeugt werden, und umgekehrt. Wieso das so ist und wieso die Verschlüsselungsmethode so sicher ist, entnehmen Sie bitte Kapitel 5.
Nun aber genug der Belehrungen und zurück zum eigentlichen Thema.
Starten Sie Kgpg durch das Drücken von Alt + F2 oder aus der Konsole heraus und der Eingabe von „kgpg“. Klicken Sie nun in der Werkzeugleiste auf „Schlüssel verwalten“.



In dem sich öffnenden Fenster müssen Sie nur noch auf die Schaltfläche „Schlüsselpaar generieren“ klicken:

Sie werden nun aufgefordert Ihren Namen einzugeben, anschließend noch Ihre E-Mail-Adresse (natürlich die, von der aus Sie verschlüsseln bzw. signieren wollen), dann eventuell ein Kommentar, wie „Geschäftspost“ oder „Privatpost“, und schließlich nach einem Klick auf OK die Passphrase oder das Verschlüsselungspasswort, was in der GPG-Sprache und im Folgenden „Mantra“ genannt wird.

Zum Mantra ein kleiner Exkurs. Weitere Informationen darüber finden Sie bei den Links in Kapitel 5:

- wichtig ist, dass das Mantra nicht leicht erraten werden kann. So sollte es auf keinen Fall Ihren Namen, Spitznamen oder sonstige Informationen, die jeder weiß, enthalten. Geburtsdaten sind ebenfalls „out“.
- Das Mantra sollte möglichst lang sein; je nach Gehirnkapazität und Faulheit nicht allzu lang! Mindestens 10 Zeichen sollte es schon haben, denn je länger ein Passwort und je komplizierter die Zeichen sind, desto schwerer und umständlicher ist es zu knacken bzw. zu erraten.
- Verwenden Sie am besten einen Passwortsatz, der Ihnen vertraut ist. Nehmen wir mal an, Sie wollen „AllemeineEntchen“ verwenden. Dass jeder darauf kommen kann, ist klar, darum müssen Sie sich etwas einfallen lassen. Wie wäre es mit: „AllMeiEnt“ oder kombiniert mit Ihrem Geburtsjahr in umgekehrter Reihenfolge „82AllMeiEnt19“? So können Sie jedes Mal Ihr Mantra aus diesem Satz ableiten. Seien Sie kreativ und stellen Sie Ihre eigenen Regeln auf, die keiner erraten kann! Bauen Sie Zahlen und Sonderzeichen ein (vorsicht bei deutschen Buchstaben wie ü, ä und ö – im Urlaub kann das zum Verhängnis werden).
- Sagen Sie keinem Ihr Passwort, denn dann sind es nicht mehr Ihre persönlichen Mails, sondern auch die des Partners etc.
- Prägen Sie sich das Passwort gut ein (am besten leicht ableitbar – aber nicht zu leicht für andere). Kommen Sie gar nicht auf die Idee, Ihr Mantra aufzuschreiben und eventuell auf die Tastatur zu kleben! Bei Verlust des Notizzettels oder durch eine neugierige Schwester, die unbedingt mal die persönlichen Sachen durchwühlen muss, hat man einen oder mehrere Mitleser mehr!

Ist nun ein perfektes Mantra gefunden, muss es zwei mal eingegeben und auf „OK“ geklickt werden. Es dauert nun einige Zeit, bis der Computer Ihren persönlichen Schlüssel errechnet. Wenn Sie auf „Fertig“ klicken, haben Sie Ihren ersten persönlichen Schlüssel erzeugt. Dieser erscheint nun in der Liste.
Wollen Sie nun Ihre ersten signierten Mails verschicken, dann können Sie in Kapitel 3 weiter lesen. Wenn Sie jedoch eine Mail verschlüsseln wollen, müssen Sie aber weiter lesen.

2.2 Öffentliche Schlüssel importieren

Wie schon gesagt, brauchen Sie einen öffentlichen Schlüssel, um E-Mails verschlüsseln zu können bzw. um eine Signatur zu überpüfen. Wollen Sie zum Beispiel an mich eine verschlüsselte E-Mail schicken, benötigen Sie dazu meinen öffentlichen Schlüssel. Doch wie kommen Sie an ihn heran bzw. an andere öffentliche Schlüssel?
Hierzu gibt es unterschiedliche Möglichkeiten, die hier kurz erläutert werden:

- Sie bekommen eine E-Mail, an der der öffentliche Schlüssel angehängt ist. Meistens ist es eine kleine Datei mit der Endung „asc“
- Sie bekommen eine Diskette (oder ein sonstiges Medium) auf der sich der öffentliche Schlüssel als Datei befindet
- Sie nutzen einen sogenannten Keyserver, auf dem Sie den Schlüssel zu der gewünschten Person suchen. Keyserver sind öffentlich zugängliche Server, die sehr viele öffentliche Schlüssel von unterschiedlichen Leuten beinhalten. Man kann sich die betreffende Person mit Hilfe eines Suchformulares anzeigen lassen.
  Adressen zu Keyservern finden Sie in Kapitel 5.

Haben Sie nun meinen Schlüssel? Öffnen Sie mal die Datei... sie sieht in etwa so aus:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (GNU/Linux)

mQGiBD28RbYRBAC7e6NTsxEmzRkwarJNK9zWrqHZjGMJxnrh1FmaRr05lyyzkcvD
EXmuV3v3qjsrWtF/4Wy36dMyrJHnYjFvrMZ1abaExPk24MHQZSi9vgvZbwTGioR+
[...]
Rd8ACgkQWkuo0WcTQgem5wCeLduOXIZ0141oRazzCJUuxiZN4wgAnRDbSo54xEGm
ERXbKaA78e/JtPXn
=nSsp
-----END PGP PUBLIC KEY BLOCK-----
```

Nun ist es an der Zeit, diesen Schlüssel an seinen Schlüsselbund zu heften, um künftig überprüfen zu können, ob meine Mail auch wirklich von mir ist, oder aber um verschlüsselte Mails an mich zu schicken.

Starten Sie dazu Kgpg, klicken Sie auf die Schaltfläche „Schlüssel verwalten“ (siehe oben) und dann auf „Schlüssel importieren“:

Wählen Sie die Datei (also den Schlüssel) im Dateidialog aus. Haben Sie einen Schlüssel ausgewählt, klicken Sie auf OK und dieser erscheint nun in der Schlüsselliste.

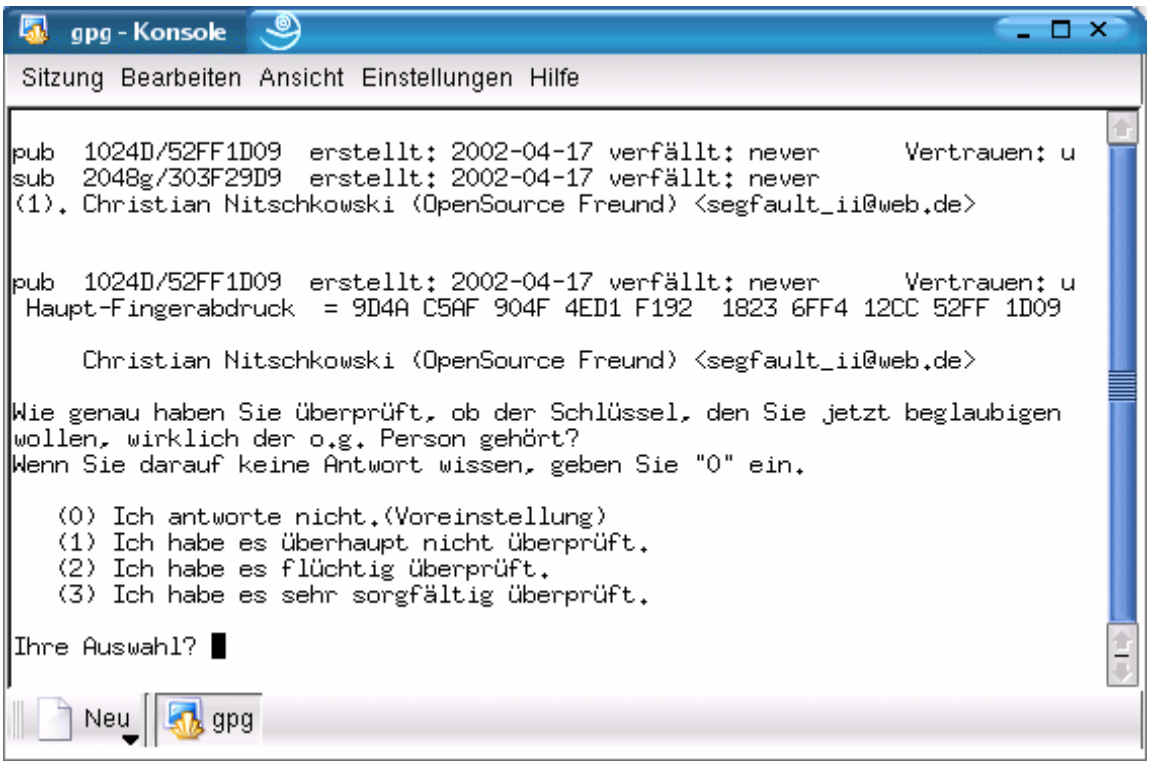
2.3 Öffentlichen Schlüsseln vertrauen

Woher wissen Sie eigentlich, dass der Schlüssel, auf dem „Gregor Waluga“ draufsteht, auch wirklich von mir stammt? Es könnte sich ja einer den Scherz erlaubt haben und mit einer völlig fiktiven E-Mail-Adresse aber meinem Namen einen Schlüssel erzeugt haben, den er nun verbreitet!
Auch dieses Problem lässt sich einfach beheben. Es scheint lästig zu sein, aber was tut man nicht alles für die Sicherheit...
Drum sollte man sich auf jeden Fall vorher per Mail, Telefon oder persönlichem Gespräch über die Herkunft des Schlüssels informieren. Haben Sie sich überzeugt, dass der Schlüssel, den Sie importiert haben, auch wirklich der des Kommunikationspartners ist, müssen Sie ihn mit Ihrem öffentlichen Schlüssel signieren.

Doch wieso das Ganze? Zum einen haben Sie nun die Gewissheit, dass der Schlüssel echt ist, zum anderen können Sie nun verschlüsselte Botschaften per E-Mail verschicken. KMail würde an dieser Stelle Schluss machen, da er nur signierte Schlüssel zum Verschlüsseln benutzt! Also sind Sie auch von der technischen Seite her gezwungen, jeden Schlüssel zu überprüfen... doch nicht nur Sie können einem Schlüssel vertrauen, auch andere können den Schlüssel zuvor signiert haben. Das zeigt Ihnen, dass man der Person wirklich vertrauen kann. So entsteht nach und nach ein „Netz des Vertrauens“, da die GnuPG-Mitglieder untereinander sich das Vertrauen aussprechen.
Bereits signierte Schlüssel bekommen Sie meistens von Keyservern oder aber auch von Freunden bzw. Bekannten Ihres Kommunikationspartners.

Um nun die Echtheit des gerade importierten Schlüssels zu bekunden, klicken Sie einfach auf den öffentlichen Schlüssel Ihres Kommunikationspartners und dann in der Werkzeugleiste auf „Schlüssel signieren“:

Wählen Sie anschließend einen Ihrer Schlüssel aus, mit dem der fremde Schlüssel signiert werden soll. Dann erscheint ein Bestätigungsfenster, in dem Sie entweder „Ja“ oder „Nein“ auswählen. Nach einem Klick auf „OK“ müssen Sie Ihr Mantra eingeben. Es erscheint dann ein Konsolenfenster und sieht in etwa so aus:



So signiert man mit Kgpg importierte, öffentliche Schlüssel

Hier werden nun allgemeine Informationen über den zu unterzeichnenden Schlüssel angezeigt. Sie werden nochmals aufgefordert, den Schlüssel auf jeden Fall zu überprüfen. Wählen Sie nun eine der möglichen Aussagen aus und geben die entsprechende Ziffer ein. Nach einem Druck auf die Eingabetaste müssen Sie nun, um die Signierung abzuschließen, ein „ja“ eingeben (oder eben „nein“).

Kgpg lässt Sie aber auch das so genannte „Benutzervertrauen“ festlegen. Markieren Sie den gewünschten Schlüssel in der Liste und klicken Sie in der Werkzeugleiste auf „Schlüssel editieren“. Es erscheint ein Konsolenfenster. Geben Sie in der Eingabeaufforderung ein „trust“ ein. Wählen Sie nach Ihrer persönlichen Einschätzung eine Vertrauensmethode aus und geben Sie die entsprechende Ziffer ein.
Zwingend ist die Vergabe eines Benutzervertrauens nicht, daher ist es hier nur flüchtig beschrieben.
Das Benutzervertrauen wird später im E-Mailfenster von KMail angezeigt.

2.4 Schlüssel exportieren bzw. sichern

Wenn Sie mal ein neues Sytem aufsetzen wollen, oder einfach Ihre Daten sichern wollen, sollten Sie auch an Ihre Schlüssel denken! Dazu gibt es zwei Möglichkeiten: Entweder Sie exportieren die Schlüssel einzeln mit Kgpg oder kopieren bzw. sichern das Verzeichnis, in dem die Schlüssel gespeichert sind.
Wenn Sie einen öffentlichen Schlüssel mit Kgpg exportieren wollen, öffnen Sie einfach die Schlüsselverwaltung und klicken auf den zu exportierenden Schlüssel. Anschließend klicken Sie in der Werkzeugleiste auf „Öffentlichen Schlüssel exportieren“:

Wählen Sie dann einen Dateinamen aus und klicken dann auch „Speichern“. Mit dieser Methode können Sie

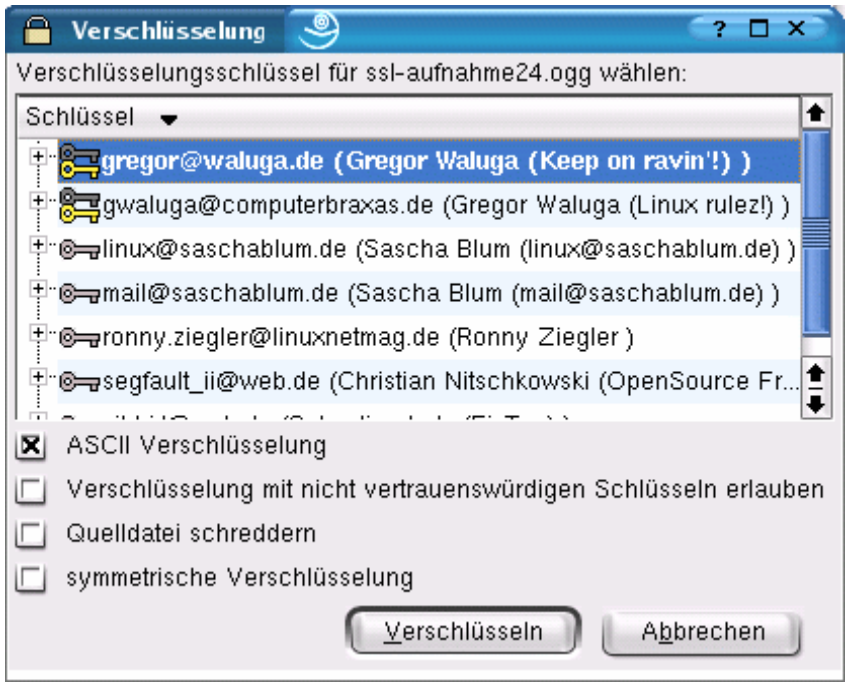
aber nur öffentliche Schlüssel exportieren.
Um auch Ihre privaten Schlüssel zu exportieren, die Sie zur Verschlüsselung benötigen, müssen Sie auf den privaten Schlüssel mit der rechten Maustaste klicken und „Geheimen Schlüssel exportieren“ auswählen:

Wenn Sie alle Schlüssel auf einmal (jedoch nicht einzeln) sichern wollen, müssen Sie den Ordner kopieren, in dem sich die Schlüssel befinden. Normalerweise finden Sie es in Ihrem Homeverzeichnis im versteckten Unterordner „.gnupg“ (also z.B. „/home/benutzer/.gnupg/“). Es befinden sich darin auch versteckte Dateien!

Anmerkung: Insbesonders, wenn Sie private Schlüssel z.B. auf Disketten sichern, müssen Sie sich darüber im Klaren sein, dass es ein großes Sicherheitsrisiko ist! Es kann zwar ohne Passwort nur bedingt genutzt werden, trotzdem wäre es möglich, den Schlüssel zu cracken und ihn unrechtmäßig zu verwenden! Darum sollten Sie Ihre privaten Schlüssel immer sicher aufbewahren!

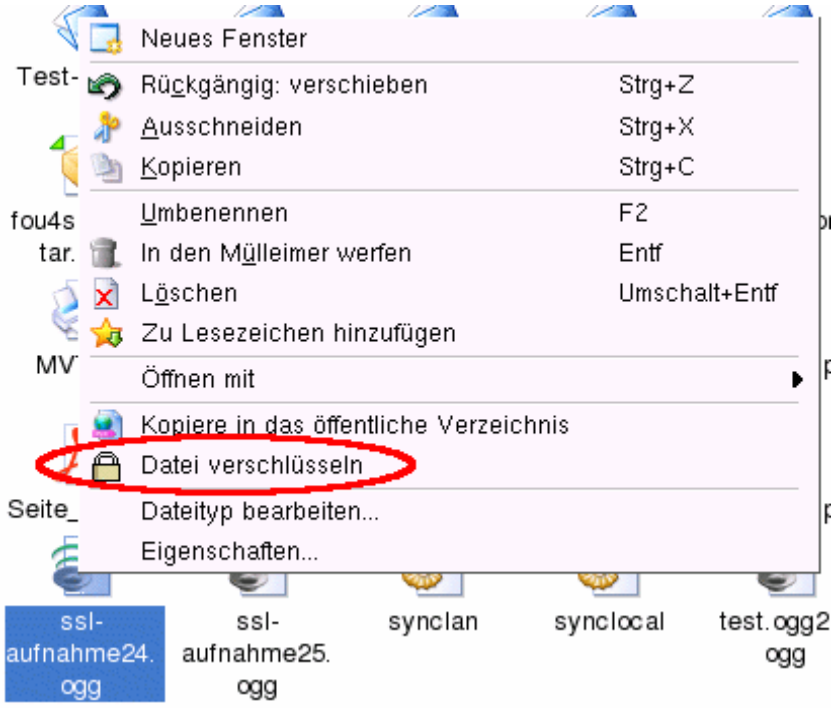
2.4 Dateien signieren und verschlüsseln

Auch wenn dieses Thema erst später besprochen werden sollte, passt es doch sehr gut zu diesem Kapitel, und soll Ihnen eine neue Möglichkeit eröffnen, persönliche Daten in Form von Dateien sicher zu versenden.
Dazu gibt es in Kgpg eine Möglichkeit, beliebige Dateien zu signieren oder aber zu verschlüsseln. Es ist eigentlich das selbe Prinzip, wie bei den E-Mails (vergleiche dazu Kapitel 4): Sie verschlüsseln eine Datei mit Ihrem privaten und dem öffentlichen Schlüssel des Partners und nur er kann die Datei wieder entschlüsseln.
Wenn Sie Dateien verschlüsseln wollen, klicken sie in Kgpg im Menü auf „Datei“ und dann auf „Datei verschlüsseln...“. Es öffnet sich ein Dateidialog, in dem Sie die Datei auswählen, die verschlüsselt werden soll. Dann einfach auf „OK“ klicken und schon erscheint folgendes Fenster:



Schlüsselauswahl für die Dateienverschlüsselung

Hier wählen Sie den Verschlüsselungsschlüssel aus und klicken auf „Verschlüsseln“. Mit einem Dateimanager, wie etwa dem Konqueror, sehen Sie im selben Verzeichnis eine Datei, mit dem selben Namen. Wenn Sie genauer hinsehen, stellen Sie fest, dass das Programm einen neue Endung „gpg“ angehängt hat. Es zeigt, dass es sich um eine verschlüsselte Datei handelt.
Kgpg unterstützt auch eine tolle Möglichkeit, mit der Sie Dateien direkt aus dem Konqueror heraus verschlüsseln können. Klicken Sie dazu einfach mit der rechten Maustaste auf die Datei. Es erscheint ein Kontextmenü und wählen Sie dort „Datei verschlüsseln“ aus:



Die Dateiverschlüsselung direkt aus dem Konqueror heraus

Anschließend werden Sie aufgefordert den Schlüssel auszuwählen, der verwendet werden soll. Kurze Zeit später erscheint die Datei mit der Endung „gpg“ im Konqueror.

Wenn Sie eine Datei signieren, hat diese später die Endung „sig“. Um dies zu tun, klicken Sie im Menü auf „Signatur“ und weiter auf „Signatur generieren“. Es erscheint ein Dateidialog in dem Sie die Datei auswählen. Wenn Sie auf „OK“ klicken, müssen Sie nur noch Ihren Schlüssel, mit dem signiert werden soll, auswählen und dann ihr Mantra eingeben.
Generiert wird eine kleine Datei, die Sie mit Ihrer Ursprungsdatei verschicken oder auf Ihre Webseite tun.

Zum Entschlüsseln müssen Sie in Kgpg im Menü auf „Datei“ und auf „Datei entschlüsseln...“ klicken. Laden Sie im Dateidialog die verschlüsselte Datei und klicken auf „OK. Anschließend müssen Sie nur den Pfad und die Datei bestimmen, in die entschlüsselt werden soll. Dann nur noch das Mantra eingeben, und schon ist die Datei wieder da.

Um eine Signatur zu überprüfen, gehen Sie im Menü auf „Signatur“, dann auf „Signatur überprüfen“. Wählen Sie die Signaturdatei oder die Datei, zu der die Signatudatei gehört, aus und klicken dann auf „OK“. Es erscheint ein Fenster, in dem steht, ob die Signatur korrekt ist, oder gebrochen wurde.

3. KMail konfigurieren

So richten Sie KMail ein, um möglichst komfortabel E-Mails signieren oder verschlüsseln zu können.

3.1 OpenPGP richtig und komfortabel einstellen

Der normale Computeranwender meint immer, es sei so umständlich E-Mails zu verschlüsseln, es gehe so viel Zeit drauf... dabei ist es ihr gutes Recht Ihre Mails sicher auf die Reise zu schicken. Als KMail-Anwender haben Sie ein ideales Werkzeug in die Hand bekommen! Mit nur wenigen Einstellungen können Sie zukünftig mit einem minimalen Zeitaufwand, sicher kommunizieren. Auch ich habe nie geglaubt, wie einfach es ist. Nach folgenden drei Schritten, die auch im Detail erläutert werden, sind Sie startklar:

Zuerst müssen Sie KMail starten. Dann gehen Sie in das Menü „Einstellungen / KMail einrichten... / Sicherheit / OpenPGP“ und schon haben Sie die Schaltzentrale vor sich. Im Folgenden sind die Punkte näher erläutert:

- Wählen Sie unter „Verschlüsselungsprogramm“ das Program aus, das Sie verwenden, also „GnuPG – GNU Privacy Guard“
- Bei den folgenden Optionen stellen Sie das Verhalten von GnuPG ein, inwieweit es mit KMail zusammenarbeitet und wieviel Arbeit es Ihnen abnimmt. Gleich vorweg: Komfortabilität geht auf Kosten der Sicherheit! Näheres dazu bei den entsprechenden Punkten:
    - „Passwort im Speicher halten“: Normalerweise müssten Sie ihr Mantra bei jedem Signieren, bei jedem Ver- und Entschlüsseln eingeben; vor allem bei längeren Passwortsätzen kann das schnell lästig werden. Darum können Sie das Passwort auch im Speicher halten lassen, was so viel heißt, dass Sie nur einmal Ihr Passwort eingeben müssen. Bei Bedarf wird das Passwort aus dem Speicher ausgelesen – eine erneute Eingabe entfällt. Doch hier ist der Knackpunkt: Trotz aller Vorsicht beim Programmieren der Software und dieser Option, kann es unter Umständen dazu kommen, dass ein Cracker – wie auch immer – an ihr Mantra im Speicher kommen kann, vor allem wenn Sie im Internet sind. Es ist relativ unwahrscheinlich, dass jemand ohne Ihr root-Passwort Ihren Speicher per Internet auslesen kann, aber es sei lieber gewarnt, denn eine 100 %ige Sicherheit kann es nicht geben! Wenn Sie KMail beenden, wird auch das Passwort aus dem Speicher gelöscht.
    - „Zusätzlich eigenen Schlüssel verwenden“: Wenn Sie eine Nachricht verschlüsseln, brauchen Sie den öffentlichen Schlüssel des Empfängers und Ihren privaten Schlüssel. Nur der Empfänger kann die Mail entschlüsseln, da nur sein privater Schlüssel zu seinem öffentlichen Schlüssel passt. Haben Sie was bemerkt? Was ist wenn SIE die Mail nochmal lesen wollen? Genau: Sie können diese nicht mehr wieder öffnen, da Sie die Mail nur mit dem öffentlichen Schlüssel des Empfängers verschlüsselt haben! Ihr privater Schlüssel taugt da auch nicht viel, denn der private Schlüssel muss auf den öffentlichen (passenden) Schlüssel treffen, um die Mail wieder entschlüsseln zu können.
      Diese Option verschlüsselt Ihre Mail zusätzlich noch mit Ihrem eigenen öffentlichen Schlüssel, damit auch Sie im Falle einer Korrektur oder einem Wieder-Lesen die Mail entschlüsseln können.
      Auch hier ist etwas Vorsicht geboten: Haben Sie die Option „Passwort im Speicher halten“ aktiviert, könnte bei Ihrer Abwesenheit am Rechner ein Dritter Ihre bereits verschickten verschlüsselten E-Mails lesen.
    - „Nach Erstellung chiffrierten/signierten Text anzeigen“: Nach jedem Verschlüsselungs- oder Signaturvorgang wird der Text in einem extra Fenster im Klartext angezeigt. So kann man überprüfen, ob der Vorgang erfolgreich war. Laut KMail-Handbuch sollte man diese Option aktiviert lassen.
    - „Wahl des Schlüssels für die Verschlüsselung immer bestätigen lassen“: Vor dem Versand wird der Benutzer gefragt, welchen Schlüssel er für den Verschlüsselungsvorgang verwenden will. Wenn diese Funktion deaktiviert ist, wird man nur gefragt, wenn kein passender Schlüssel für den Empfänger gefunden werden konnte.

Kommen wir zum zweiten Punkt. Gehen Sie nun im offenen Fenster auf „Nachricht erstellen“. Bei „Allgemein“ stehen Ihnen nun zwei Optionen zur Verfügung, die etwas mit unserem Thema zu tun haben:

- „Nachrichten automatisch mit OpenPGP signieren“: Ich persönlich habe dieses Feld aktiviert. Hier werden alle von Ihnen geschriebenen Mails automatisch signiert. Was das Signieren eigentlich ist, erfahren Sie in 4.1 in dieser Anleitung.
- „Nachrichten möglichst automatisch verschlüsseln“: Wird ein öffentlicher Schlüssel des Empfängers gefunden, werden die an Ihn gerichteten Mails automatisch verschlüsselt.

Und schon sind wir beim dritten und letzten Punkt angelangt! Gehen Sie nun zu der Einstellung der „Identität“. Wählen Sie die E-Mail-Adresse aus, von der aus Sie signierte bzw. verschlüsselte Mails verschicken wollen (normalerweise Identität „Standard“).
Gehen Sie nun im Registerreiter unten auf „Erweitert“. Klicken Sie nun neben dem Feld für „OpenPGP-Schlüssel“ die Schaltfläche „Ändern...“. Ein Fenster mit dem Titel „Eigener OpenPGP-Schlüssel“ erscheint. Hier können Sie nun, passend für Ihre E-Mail-Adresse, den eigenen Schlüssel auswählen. Je nachdem wieviele Schlüssel Sie für welche E-Mail-Adresse angelegt haben (vergleiche 2.1) ist die Liste entsprechend lang. Wählen Sie natürlich den Schlüssel für die gerade eben gewählte Identität aus (E-Mail-Adressen müssen logischerweise übereinstimmen).

Damit sind wir nun mit dem Einstellen von KMail für die Verwendung von GnuPG fertig. Hier vielleicht noch eine kleine Aufstellung zwischen Sicherheit und Komfortabilität:

nötige Einstellungen		**Sicherheit**	**Komfortabilität**
Einrichtungsfeld „Sicherheit“	Passwort im Speicher halten	nein	ja
	Zusätzlich eigenen Schlüssel verwenden	nein	eigenes Ermessen
	Nach Erstellung chiffrierten / signierten Text anzeigen	ja	nein
	Wahl des Schlüssels für die Verschlüsselung immer bestätigen lassen	ja	nein
Einrichtungsfeld „Nachrichten erstellen“	Nachrichten automatisch mit OpenPGP signieren	ja	eigenes Ermessen – Empfehlung: ja
	Nachrichten möglichst automatisch verschlüsseln	ja	eigenes Ermessen – Empfehlung: nicht unbedingt nötig

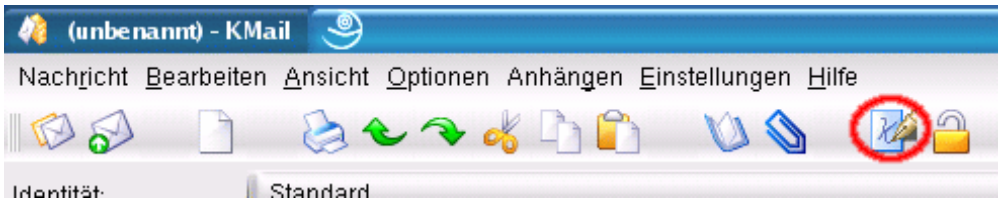
4. Jetzt geht's los

Nach der ganzen Theorie und den vielen Vorbereitungen kommen wir nun endlich dazu, unsere signierten oder verschlüsselten Mails versandfertig zu machen.

4.1 E-Mails signieren

Beim Signieren von Mails wird automatisch der voreingestellte Schlüssel für Ihre Identität genommen, den Sie in Kapitel 3.1 beim Punkt drei eingestellt haben.
Sollten Sie, ebenfalls in Kapitel 3.1 – zweiter Punkt, Ihre E-Mail immer automatisch signieren lassen, brauchen Sie nichts weiter zu tun, außer auf „Neue Nachricht“ zu klicken und Ihre E-Mail ganz normal zu verschicken. Je nach gewählten Einstellungen (Passwort eingeben oder aus dem Speicher holen) geht es mehr oder weniger schnell und schon haben Sie Ihre erste signierte Nachricht verschickt.

Ansonsten müssen Sie bei einer „manuellen Signierung“ nur einen Schritt dazwischen schieben. Und zwar müssen Sie im Mailfenster lediglich auf das hervorgehobene Zeichen klicken, das für das Signieren von Mails steht:



Ein Klick auf diese Schaltfläche signiert die Mail

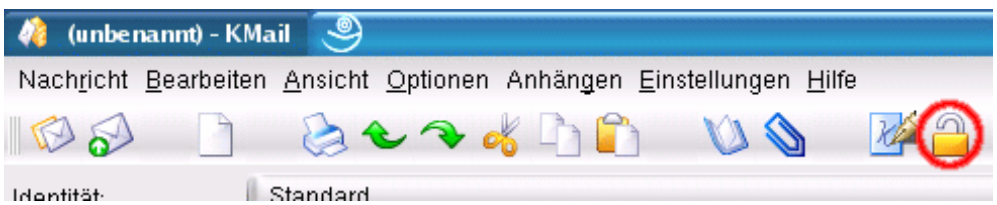
Ansonsten haben Sie es nun geschafft und soeben Ihre erste signierte E-Mail verschickt.

Was aber ist das Signieren? Die soeben verschickte E-Mail wurde in einen Umschlag gepackt, der sich aus einer sogenannten MD5-Prüfsumme, die mit Hilfe Ihres privaten Schlüssels errechnet wurde, zusammensetzt. Das heißt soviel, dass der Empfänger mit Ihrem öffentlichen Schlüssel (er muss ihn vorher haben) erkennen kann, dass der Umschlag samt Inhalt von Ihnen kommt. Wurde die Signatur während des Transportes gebrochen, wird dies in KMail anhand eines roten Rahmens deutlich gemacht. Dann können Sie auch davon ausgehen, dass jemand seine Nase in die Mail gesteckt hat oder diese sogar verändert hat!
Als praktisches Beispiel kann man sich in der realen Welt einen Umschlag nehmen und ein Sticker auf den Verschluss draufkleben. So sieht der Empfänger, ob jemand den Brief aufgemacht hat, oder nicht. Weitere Informationen zur Signatur finden Sie in Kapitel 5.

Hinweis: Eine Signatur kann nur überprüft werden, wenn das E-Mailprogramm das auch unterstützt! So wird bei einem Bekannten, der Outlook Express ohne PGP-PlugIn verwendet, die Signatur auch nicht überprüft und die Mail wird wie folgt eingeleitet: -----BEGIN PGP SIGNED MESSAGE-----

4.2 E-Mails verschlüsseln

Das Vorgehen ist praktisch das selbe, wie in 4.1, mit dem Unterschied, dass Sie auf ein anderes Icon klicken müssen:



Ein Klick auf diese Schaltfläche verschlüsselt die Mail

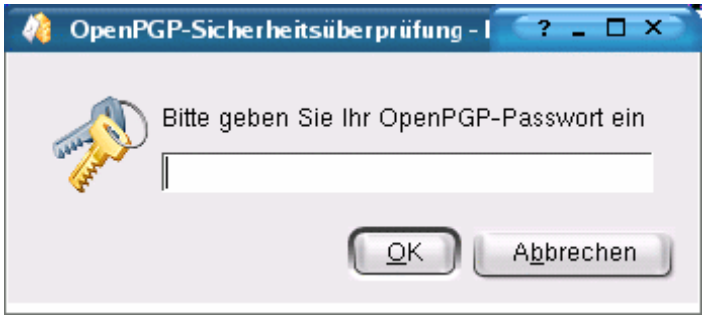
Klicken Sie nun auf „In Postausgang“ und schon geht die Post ab. :-) Vorher müssen Sie aber noch den öffentlichen Schlüssel Ihres Korrespondenzpartners wählen. Sie müssen dies nur einmal machen, wenn Sie

in Kapitel 3.1, Punkt 1, die Option „Wahl des Schlüssels für die Verschlüsselung immer bestätigen lassen“ deaktiviert haben und zusätzlich die Option „Immer mit diesem Schlüssel verschlüsseln“ (im Auswahlfenster des Schlüssels) wählen.
Sie können natürlich auch beide Icons anklicken, dann wird die E-Mail sowohl signiert, als auch noch zusätzlich verschlüsselt.
Anmerkung**:** Je nach verwendeter Version von KMail oder verwendetem Theme von KDE, können die beiden Schaltflächen anders aussehen.

Das Signieren kenne ich, aber wo ist der Unterschied zum Verschlüsseln? Das Verschlüsseln ist praktisch eine Steigerung vom Signieren. Hier wird die Nachricht nicht in einen Umschlag gesteckt, sondern in eine Geheimsprache übersetzt. Diese Geheimsprache errechnet der Computer aus Ihrem privaten Schlüssel und dem öffentlichen Schlüssel des Empfängers. Dieser kann den Text nur dechiffrieren, wenn sein privater Schlüssel mit seinem öffentlichen in der Mail zusammenpasst. Wer also nicht den privaten Schlüssel des Empfängers hat, kann die E-Mail auch nicht entschlüsseln.
Wer wissen will, wie genau die Verschlüsselungstechnik funktioniert, kann sich mal in Kapitel 5 umschauen.

4.3 E-Mails entschlüsseln

Sie können entweder Ihre eigene, verschlüsselte E-Mail wieder entschlüsseln (es sei denn Sie haben in 3.1 den eigenen Schlüssel nicht verwendet), oder eine, die Ihnen von einem Kommunikationspartner zugesandt wurde.
Wenn Sie auf eine solche verschlüsselte E-Mail klicken, fragt Sie KMail automatisch nach Ihrem Mantra:



KMail fragt Sie nach Ihrem Mantra

Haben Sie es korrekt eingegeben, wird die Mail entschlüsselt und wie gewohnt angezeigt.

KMail hat dieses wunderbare Feature, dass signierte und / oder verschlüsselte Nachrichten, die von Ihrem Kommunikationspartner zugesendet wurden, in unterschiedlichen Rahmen und unterschiedlicher Hintergrundfarbe dargestellt werden.

	Zustand	**Farbe des Rahmens**
Signierte E-Mail	Gültige und vertraute Signatur	grün
	Gültige aber nicht vertraute Signatur	gelb
	Ungültige Signatur	rot
Verschlüsselte E-Mail	Entschlüsselt	blau
Signierte und verschlüsselte E-Mail	Entschlüsselt; gültige und vertraute Signatur	blau und grün
	Entschlüsselt; gültige aber nicht vertraute Signatur	blau und gelb
	Entschlüsselt; ungültige Signatur	blau und rot

Eigentlich sind wir nun mit der Theorie und der Anleitung fertig.
Herzlichen Glückwunsch! Nun können Sie einfach und sicher kommunizieren!

5. Hinweise und weitere Informationen

Wer intensiver in die Materie einsteigen will, kann sich mal auf folgenden Internetseiten umschauen:

http://www.gnupg.org	Natürlich die erste Adresse, die sich genaustens mit GnuPG und der Verschlüsselung beschäftigt
http://www.sicherheit-im-internet.de	Eine von der Bundesregierung liebevoll aufbereitete Internetseite, die sich allgemein mit der Sicherheit im Internet beschäftigt. Ein GnuPP-Paket (Anleitung und CD-ROM) kann dort auch kostenlos bestellt bzw. heruntergeladen werden. Auf der Silberscheibe ist die PDF für Durchblicker drauf (siehe unten).
http://www.uni-koeln.de/rrzk/kompass/94/k944a.html	Eine wissenschaftlich orientierte Anleitung über die Verschlüsselung. Mit tollen Bildchen! ;-)
http://www.keyserver.net	Hier kann man nach PGP-Schlüsseln suchen

Darüber hinaus kann ich auch ein Buch vom Bundesministerium für Wirtschaft und Technologie empfehlen, das ich selber dazu genutzt habe, mich in das Thema hineinzuarbeiten. Es beschreibt auf deutsch und sehr verständlich, was die Verschlüsselung ist, wozu man sie braucht, wie man sie anwendet und wie sie mathematisch-technisch funktioniert. Dieses Buch steht unter der GNU Free Documentation License und kann unter folgender Adresse kostenlos als PDF bezogen werden:

GnuPP für Einsteiger-Broschüre (kann auch kostenlos bestellt werden – siehe oben)	http://www.sicherheit-im-internet.de/download/einsteiger.pdf
DIE Empfehlung, wer wirklich mehr darüber wissen will. Sehr einfach geschrieben und sehr ausführlich!	http://www.sicherheit-im-internet.de/download/durchblicker1.1.pdf

Danksagungen:

Ich sage Dank für die Unterstützung von **Christian Nitschkowski**. Er hatte mir die ersten signierten Mails geschickt und dadurch kam ich mit diesem Thema zum ersten Mal in Berührung. Auf eine Nachfrage, was denn der gelbe Rahmen sei, schickte er mir eine längere Anleitung mit einer Erklärung, wie das Verschlüsseln geht. Ich habe ihn so lange genervt [Sorry ;-)], bis GnuPG und GPA liefen. Mein OpenOffice, um dieses Tutorial zu schreiben, habe ich übrigens mit seinem Programm gestartet (http://segfaultskde.berlios.de/index.php?content=oooqs).

Dann ebenfalls ein Dankeschön an **Sascha Blum**, der sich das Ganze hier mal durchgelesen hat um nach Fehlern Ausschau zu halten und seine Verbesserungsvorschläge preis zu geben. Außerdem musste er meine tausenden Testmails über sich ergehen lassen. Dafür kann er jetzt auch sicher kommunizieren! ;-)

Danke auch an meine **Zivistelle**. Bei der Aufsicht im Schwimmbad hatte ich genug Zeit, um mir in aller Ruhe die Broschüre vom Bundesministerium für Wirtschaft und Technologie über das GnuPP (GNU Privacy Project) durchzulesen. ;-) Die Basis für das Wissen, das ich im Tutorial niedergeschrieben habe.

Diese Anleitung wurde nach bestem Wissen und Gewissen geschrieben. Sollten dennoch Fehler enthalten sein, so bitte ich, mir diese mitzuteilen. Für Schäden an Hard- und Software sehe ich mich nicht verantwortlich.