GnuPG im Alltagsgebrauch

Autor: Mike Ashley ()
Layout: Matthias Hagedorn (*matthias.hagedorn@selflinux.org*)

Inhaltsverzeichnis

1 dailyuse

GnuPG ist nicht nur eine komplexe Software, sondern es gibt auch einige technische, gesellschaftliche und rechtliche Aspekte, die berücksichtigt werden sollten:

Auf diese Aspekte wollen wir im folgenden eingehen.

* Technisch muß es verschiedenen Situationen mit drastisch unterschiedlichen Sicherheitsanforderungen gerecht werden, was die Schlüsselverwaltung kompliziert.
* Die Benutzung von GnuPG ist nicht unbedingt eine rein persönliche Entscheidung. Um GnuPG effektiv nutzen zu können, müssen beide miteinander kommunizierenden Seiten es benutzen.
* Die Haltung der Gesetzgeber zur elektronischen Verschlüsselung und zu digitalen Signaturen unterscheidet sich von Land zu Land. Insbesondere die Frage einer legalen Benutzung von GnuPG bzw. Verschlüsselung im allgemeinen steht gegenwärtig bei vielen nationalen Regierungen zur Debatte.

2 Definition Ihres Sicherheitsbedarfs

Einer der wichtigsten Gründe, GnuPG zu benutzen, ist der Schutz Ihrer Privatsphäre. Das bedeutet, daß Sie mit anderen korrespondieren können, ohne daß Dritte die Möglichkeit haben, mitzulesen, und daß Sie vertrauliche Daten auf Ihrem Rechner dem unbefugten Zugriff anderer entziehen können. Ebenso gibt Ihnen GnuPG die Möglichkeit, Ihre Daten (E-Mail) durch digitale Signaturen zu authentifizieren und deren Integrität zu sichern.

Wie Sie GnuPG benutzen, sollte von der Zielstrebigkeit und Findigkeit derer abhängen, die unerlaubt Ihre verschlüsselten Nachrichten mitlesen wollen. Ein solcher **Lauscher** kann ein neugieriger Systemadministrator sein, der Ihre E-Mails mitliest, es könnte ein Industriespion sein, der versucht, Ihre Firmengeheimnisse auszuspähen, oder es könnte die Staatsanwaltschaft sein, die Ihnen auf den Fersen ist. Wenn Sie GnuPG benutzen, um mehr oder weniger zufälliges Mitlesen zu verhindern, wird das wahrscheinlich anders aussehen, als wenn Sie Ihre Daten gegen einen entschlossenen Angreifer schützen wollen.

Tip:

Ihr Ziel sollte es dabei sein, daß der Aufwand zur Entschlüsselung Ihrer Daten so groß wird, daß der Wert der Daten diesen Aufwand nicht mehr rechtfertigt.

Wenn Sie GnuPG auf Ihren persönlichen Gebrauch abstimmen möchten, sind vor allem vier Punkte wichtig:

* Die Wahl der Schlüssellänge Ihres öffentlichen und privaten Schlüsselpaars
* Der Schutz Ihres geheimen Schlüssels
* Die Verfallsdaten Ihrer Schlüssel und die Benutzung von Unterschlüsseln
* Der Aufbau Ihres **Web of Trust**

Eine gut gewählte Schlüssellänge schützt Sie gegen Brute-Force-Angriffe auf verschlüsselte Daten. Der Schutz Ihres privaten Schlüssels hindert einen Angreifer daran, einfach Ihren privaten Schlüssel zum Entschlüsseln von verschlüsselten Nachrichten zu verwenden und Nachrichten in Ihrem Namen zu unterschreiben. Ein sorgfältig aufgebautes **Web of Trust** verhindert, daß ein Unbefugter sich als einer Ihrer Korrespondenzpartner ausgeben kann.

> Wichtig ist die Frage, welchen Aufwand Sie entsprechend Ihren Sicherheitsanforderungen betreiben möchten, um Ihre Privatsphäre oder Ihre Firmendaten zu schützen.

3 Die Wahl der Schlüssellänge

Die Wahl der Schlüssellänge hängt von der Art des jeweiligen Schlüssels ab. Bei OpenPGP besteht ein Schlüsselbund gewöhnlich aus mehreren öffentlichen und geheimen Schlüsseln. Es sollte zumindest einen Hauptschlüssel zum Signieren und einen oder eventuell mehrere zusätzliche Unterschlüssel für die Verschlüsselung geben. Wenn man die Standardeinstellungen von GnuPG bei der Schlüsselerzeugung verwendet, ist der Hauptschlüssel ein DSA-Schlüssel, die Unterschlüssel sind ElGamal-Schlüssel.

DSA erlaubt eine Schlüssellänge bis zu 1024 Bit. Das ist angesichts der heutigen Rechenleistungen nicht besonders lang, entspricht jedoch dem Standard. Warum das so ist und warum ein DSA-Schlüssel mit 1024 Bit zur Benutzung sogar empfohlen wird, geht aus dem folgenden Absatz hervor.

ElGamal-Schlüssel andererseits können beliebig lang sein. GnuPG ist ein hybrides Verschlüsselungsverfahren mit öffentlichem Schlüssel. Der öffentliche Schlüssel wird zum Verschlüsseln eines 128-Bit-Sitzungsschlüssels benutzt, und der private Schlüssel wird zu dessen Entschlüsselung verwendet. Allerdings beeinflußt die Schlüssellänge die Ver- und Entschlüsselungsgeschwindigkeit erheblich, da der Rechenaufwand bei diesen Algorithmen exponentiell mit der Länge des Schlüssels steigt. Außerdem ist der praktische Nutzen eines großen Schlüssels trotz seiner größeren Sicherheit durchaus zweifelhaft. Wenn der Schlüssel lang genug ist, um einem Brute-Force-Angriff zu widerstehen, wird der Angreifer wahrscheinlich zu einer anderen Methode greifen, um an Ihre unverschlüsselten Daten zu gelangen. Es könnte ihm leichter fallen, in Ihre Wohnung oder Ihr Büro einzudringen oder Sie möglicherweise sogar zu überfallen. 1024 Bit sind alles in allem eine zu empfehlende Schlüssellänge. Wenn Sie wirklich einen längeren Schlüssel brauchen, dann sollten Sie ohnehin einen Fachmann in Sachen Datensicherheit konsultieren.

4 Der Schutz Ihres geheimen Schlüssels

Das Allerwichtigste bei der Benutzung von GnuPG ist der Schutz Ihres geheimen Schlüssels. Wenn jemand Ihren geheimen Schlüssel in die Hand bekommt, dann kann er damit alle für diesen Schlüssel verschlüsselten Daten entschlüsseln, und er kann digitale Unterschriften in Ihrem Namen leisten. Wenn Sie Ihren geheimen Schlüssel verlieren, sind Sie nicht länger imstande, Daten zu entschlüsseln, die für Sie verschlüsselt worden sind, und Sie können keine Unterschriften mehr leisten. Den geheimen Schlüssels zu verlieren, ist eine Katastrophe für Ihre Datensicherheit.

Egal, wie Sie GnuPG benutzen, Sie sollten die **Widerrufurkunde** des öffentlichen Schlüssels und eine Sicherheitskopie Ihres geheimen Schlüssels auf einem schreibgeschützten Datenträger - beispielsweise einer CD-ROM oder Diskette - speichern und an einem sicheren Ort aufbewahren, z. B. in einem Bankschließfach oder gut versteckt in Ihrer Wohnung. Um eventuellen Datenträgerdefekten vorzubeugen, sollten Sie vielleicht auch jeweils einen ASCII-Ausdruck (*** gpg --armor) auf Papier aufbewahren. Was immer Sie tun, die Widerrufurkunde und die Sicherheitskopie Ihres geheimen Schlüssels sollten auf Datenträger gebracht werden, die eine sichere Aufbewahrung so lange ermöglichen, wie Sie Ihren Schlüssel voraussichtlich behalten werden, und Sie sollten diese sorgfältiger aufbewahren als die Kopie Ihres täglich benutzten geheimen Schlüssels.

Als weitere Sicherheitsmaßnahme speichert GnuPG Ihren privaten Schlüssel nicht in **roher** Form ab, sondern verschlüsselt ihn stattdessen unter Benutzung eines symmetrischen Verschlüsselungsverfahrens. Deshalb brauchen Sie das **Mantra**, um mit Ihrem geheimen Schlüssel zu entschlüsseln oder zu signieren. Somit müßte ein Angreifer gleich zwei Probleme lösen, um Zugang zu Ihrem geheimen Schlüssel zu bekommen:

* Er müßte tatsächlich den Schlüssel in die Hand bekommen.
* Er müßte entweder dessen Verschlüsselung knacken oder an das Mantra kommen.

Die sichere Aufbewahrung Ihres geheimen Schlüssels ist wichtig, doch auch mit einigem Aufwand verbunden. Im Idealfall würden Sie den geheimen Schlüssel auf einem mobilen, schreibgeschützten Datenträger, wie z. B. einer Diskette, speichern und ihn auf einem nicht vernetzten Computer benutzen, zu dem nur Sie Zugang haben. Vielleicht ist das für Sie zu unbequem oder unmöglich. Vielleicht besitzen Sie auch keinen eigenen Computer und haben nur am Arbeitsplatz oder in der Schule Zugang zu einem Computer.

Das heißt aber nicht, daß Sie nun GnuPG nicht benutzen können oder sollten. Sie haben sich nur entschieden, daß Ihnen Ihre Daten zwar wichtig genug sind, um sie zu verschlüsseln, aber nicht so wichtig, daß Sie besondere Maßnahmen treffen müßten, um die erste Barriere sicherer zu machen. Es ist letztlich Ihre Entscheidung, ob Ihr Sicherheitsanspruch damit schon erfüllt ist oder nicht.

Absolut unerläßlich ist ein gutes Mantra, wenn Sie GnuPG benutzen. Jeder Angreifer, der Zugang zu Ihrem geheimen Schlüssel bekommt, muß dann noch die Verschlüsselung Ihres geheimen Schlüssels knacken. Es ist so gut wie sicher, daß ein Angreifer versuchen wird, das Mantra zu erraten, anstatt mit einem Brute-Force-Angriff den Schlüssel selbst herauszufinden.

Es ist nicht gerade leicht, sich eine ausreichend große Zahl von unzusammenhängenden Zeichen zu merken. Deshalb ist die Versuchung sehr groß, ein Mantra zu wählen, das leichter zu erraten ist als ein nach dem Zufallsprinzip erstellter 128-Bit-Schlüssel, und die meisten Leute erliegen dieser Versuchung, sodaß es für einen Lauscher besonders verlockend ist, zu versuchen, das Mantra zu erraten. Aber wenn Sie sich wirklich im klaren darüber sind, daß Sie eine Verschlüsselung schließlich deshalb benutzen, weil Sie **verhindern** möchten, daß man Ihre Daten mitlesen kann, dann werden Sie dieser Versuchung nicht erliegen und die notwendige Mühe auf sich nehmen.

Wenn das Mantra aus einem normalen Wort besteht, dann ist es ein leichtes, alle Wörter in den Wörterbüchern sämtlicher Sprachen der Welt auszuprobieren. Selbst wenn die Reihenfolge der Buchstaben oder Zeichen innerhalb des Wortes verändert worden ist, ist es immer noch leicht, Wörter aus dem Wörterbuch mit einem Katalog von Permutationen auszuprobieren. Dasselbe Problem stellt sich bei Zitaten. Im Allgemeinen sind Mantras, die auf Äußerungen der natürlichen Sprache beruhen, schlechte Mantras, da ihre Zufälligkeit gering ist und da es in der natürlichen Sprache eine Menge Redundanz gibt. Sie sollten Mantras aus der natürlichen Sprache tunlichst vermeiden.

Ein gutes Mantra ist eines, das nur sehr schwer zu erraten ist, obwohl **Sie** es sich gut merken können. Es sollte Zeichen aus der ganzen Reihe der druckbaren Zeichen auf Ihrer gesamten Tastatur enthalten. Dazu gehören auch Großbuchstaben, Ziffern und Sonderzeichen wie beispielsweise }, # oder ^.

Tip:

Seien Sie kreativ und nehmen Sie sich ein wenig Zeit bei der Wahl Ihres Mantras! Eine gutes Mantra ist wichtig für die Sicherheit Ihrer Daten und somit auch Ihrer Privatsphäre oder Firmengeheimnisse!

5 Auswählen der Verfallsdaten und Benutzung von Unterschlüsseln

Wenn Sie ein neues Schlüsselpaar erzeugen, werden standardmäßig ein DSA-Hauptschlüssel zum Unterschreiben und ein ElGamal-Unterschlüssel zum Entschlüsseln erzeugt. Dies ist von Vorteil, weil die Aufgaben der beiden Schlüssel verschieden sind und es sinnvoll sein könnte, den beiden Schlüsseln verschiedene Verfallsdaten zu geben. Der DSA-Hauptschlüssel wird benutzt, um digitale Unterschriften zu leisten, und er bestätigt Ihre Identität dadurch, daß andere ihn signiert haben. Der ElGamal-Unterschlüssel wird nur benutzt, um an Sie geschickte verschlüsselte Daten zu entschlüsseln. Typischerweise sollte eine digitale Signatur eine lange oder unbegrenzte Gültigkeitsdauer haben; Sie wollen ja auch die Unterschriften auf Ihrem Schlüssel, die Sie mühsam zusammengetragen haben, nicht verlieren. Andererseits sollte der ElGamal-Unterschlüssel in gewissen Zeitabständen gewechselt werden, um Ihre Datensicherheit zu erhöhen, da ein Angreifer, wenn der ElGamal-Unterschlüssel geknackt ist, alle Dokumente lesen kann, die für diesen Schlüssel verschlüsselt worden sind oder es noch werden.

In der Regel sollten Sie also eine unbeschränkte Gültigkeitsdauer für den DSA-Hauptschlüssel wählen. Es gibt jedoch Gründe, weshalb Sie vielleicht doch ein Verfallsdatum für Ihren Hauptschlüssel wählen sollten. Erstens kann es sein, daß Sie dem Schlüssel nur eine beschränkte Geltungsdauer geben wollen, z. B., wenn Sie den Schlüssel für ein zeitlich befristetes Ereignis wie etwa eine politische Kampagne benutzen wollen und danach nicht mehr. Ein weiterer Grund könnte in einer zusätzlichen Vorsichtsmaßnahme bestehen: Falls der Hauptschlüssel kompromittiert wird (und Sie möglicherweise auch keine Widerrufurkunde haben), würde ein Verfallsdatum den Schlüssel genau an diesem Datum unbrauchbar werden lassen.

Tip:

Einer solchen Kompromittierung sollten Sie jedoch möglichst durch Sicherheitsvorkehrungen vorbeugen, wie in 4.1.2 beschrieben.

Das Erneuern von ElGamal-Unterschlüsseln ist zwar kein Problem, kann aber unbequem werden. Kurz vor dem Verfallsdatums sollten Sie einen neuen ElGamal-Unterschlüssel erzeugen und die davon abgeleiteten öffentlichen Schlüssel bekannt geben. Diejenigen, die mit Ihnen korrespondieren wollen, müssen ja, sobald der alte Schlüssel seine Gültigkeit verliert, Ihren aktualisierten öffentlichen Schlüssel bekommen, da sie mit dem dann ungültigen Schlüssel nicht mehr verschlüsseln können. Je nachdem, wie Sie die Verteilung Ihrer öffentlichen Schlüssel organisieren, kann dies eine mühsame Angelegenheit werden. Sie müssen aber Gott sei Dank keine neuen Unterschriften einholen, um Ihren neuen Unterschlüssel zu authentisieren. Eine Unterschrift mit Ihrem authentifizierten DSA-Hauptschlüssel bestätigt die Echtheit des neuen Schlüssels.

Die erzielte zusätzliche Sicherheit mag diese Unbequemlichkeit wert sein oder nicht. Genauso wie Sie, kann ein erfolgreicher Angreifer immer noch alle Dokumente lesen, die mit einem verfallenen Unterschlüssel verschlüsselt worden sind. Das Wechseln der Unterschlüssel schützt nur Dokumente, die Sie nach diesem Wechsel verschlüsseln. Um die mit dem neuen Unterschlüssel verschlüsselten Dokumente zu lesen, müßte der Angreifer erneut in den Besitz Ihres Schlüssels **und** ihres Mantras kommen.

Es ist auch nicht nötig, mehr als einen gültigen Unterschlüssel in einem Schlüsselbund zu haben. Man erzielt keine zusätzliche Sicherheit dadurch, daß man zwei oder mehr aktive Unterschlüssel hat. Es können natürlich mehrere verfallene Schlüssel in einem Schlüsselbund sein, so daß in der Vergangenheit verschlüsselte Dokumente noch entschlüsselt werden können, doch braucht nie mehr als ein Unterschlüssel aktiv zu sein.

6 Verwaltung Ihres Web of Trust

Genauso wie beim Schutz Ihres geheimen Schlüssels müssen Sie auch bei der Verwaltung Ihres **Web of Trust** zwischen Bequemlichkeit und Sicherheit abwägen. Wenn Sie GnuPG lediglich zum Schutz gegen mehr oder weniger zufälliges Mitlesen und Dokumentenfälschungen benutzen, dann können Sie relativ vertrauensvoll hinsichtlich der digitalen Signaturen anderer Leute sein. Wenn Sie sich allerdings Sorgen machen, daß ein zu allem entschlossener Angreifer an Ihren Firmendaten oder am Eindringen in Ihre Privatsphäre interessiert ist, dann sollten Sie die Unterschriften anderer sorgfältig prüfen.

Ungeachtet Ihrer eigenen Sicherheitsbedürfnisse sollten Sie jedoch beim Unterschreiben anderer Schlüssel **immer Sorgfalt walten lassen**. Im Sinne des **Web of Trust** ist es nicht ratsam, einen Schlüssel zu unterschreiben, dessen Authentizität Sie gerade noch so weit vertrauen, wie es für Ihr eigenes Sicherheitsbedürfnis ausreichend ist. Andere, die einen höheren Sicherheitsbedarf haben, sollten sich auf Ihre Unterschrift verlassen können. Wenn man sich auf Ihre Signatur nicht verlassen kann, dann schwächt dies das **Web of Trust** und macht die Kommunikation für alle Benutzer von GnuPG schwieriger.

Tip:

Lassen Sie also beim Unterschreiben von Schlüsseln dieselbe Sorgfalt walten, die Sie von anderen auch angewandt sehen möchten, wenn Sie sich auf deren Unterschriften verlassen.

Bei der Verwaltung Ihres **Web of Trust** sollten Sie sich auf zwei Dinge konzentrieren: Einerseits auf die Frage, wessen Schlüssel Sie genügend vertrauen, um sie selber zu signieren, und andererseits auf das Abstimmen der Optionen `--marginals-needed` und `--completes-needed`. Jeder Schlüssel, den Sie persönlich signieren, wird als gültig betrachtet, deshalb ist es - außer in kleinen Gruppen - keine gute Praxis, persönlich den Schlüssel jeder Person zu unterschreiben, mit der Sie kommunizieren. Sinnvoller ist es, sich daran zu gewöhnen, den Unterschriften anderer zu vertrauen.

Es ist wahrscheinlich die beste Strategie, beim Unterzeichnen von Schlüsseln genau die Authentizität des Schlüssels bzw. die Identität des Schlüsselbesitzers zu überprüfen und ansonsten durch Optionen zu bestimmen, wie sorgfältig GnuPG bei der Authentisierung sein soll. Ein konkretes Beispiel: Sie mögen einigen wenigen engen Freunden voll vertrauen, von denen Sie wissen, daß diese beim Unterschreiben von Schlüsseln sorgfältig vorgehen; den weiteren Schlüsselbesitzern in Ihrem Schlüsselbund vertrauen Sie in dieser Hinsicht nur teilweise. Danach können Sie `--completes-needed` auf `1` und `--marginals-needed` auf `2` setzen. Wenn Sie hinsichtlich der Sicherheit stärker besorgt sind, können Sie auch die Werte `1` bzw. `3` oder `2` bzw. `3` wählen. Wenn Sie allerdings mit einem weniger großen Vertrauen hinsichtlich der Authentizität auskommen wollen und nicht so sehr mögliche Angriffe auf Ihre Privatsphäre oder Firmendaten befürchten, dann können Sie die Werte `1` und `1` einsetzen. Je höher die Werte für diese Optionen sind, desto schwieriger ist es, Ihnen einen gefälschten Schlüssel unterzuschieben.

7 Aufbau Ihres Web of Trust

Es reicht nicht aus, wenn nur Sie selbst GnuPG benutzen wollen. Um GnuPG zur sicheren Kommunikation mit anderen zu nutzen, müssen Sie ein funktionierendes **Web of Trust** aufbauen. Auf den ersten Blick scheint dies eine mühsame Aufgabe zu sein: Die Leute, mit denen Sie kommunizieren, müssen GnuPG **ebenfalls** benutzen, und die Schlüssel müssen von ausreichend vielen Personen unterschrieben sein, so daß sie als authentisch zu betrachten sind. Dies sind wohlgemerkt keine technischen Schwierigkeiten, sondern soziale. Nichtsdestoweniger müssen Sie diese Schwierigkeiten meistern, wenn Sie GnuPG benutzen wollen.

Anfangs ist es noch nicht so wichtig, daß Sie mit allen Korrespondenzpartnern sicher kommunizieren können. Wenn Sie mit dem Gebrauch von GnuPG beginnen, suchen Sie sich einen kleinen Kreis von Leuten - Sie selbst und noch ein oder zwei andere -, die ebenfalls ihr Recht auf eine geschützte Privatsphäre in Anspruch nehmen wollen. Unterschreiben Sie jeweils, wenn Sie sich von der Identität der anderen Person überzeugt haben, deren öffentlichen Schlüssel und lassen Sie sich im Gegenzug Ihren Schlüssel signieren. Dieses kleine, robuste **Web of Trust** ist Ihr Ausgangspunkt. Sie werden dessen Wert zu schätzen lernen und - wenn Sie Ihr **Web of Trust** in der Zukunft weiter ausbauen - um so gewissenhafter und vorsichtiger sein.

Über Ihr anfängliches **Web of Trust** hinaus möchten Sie wahrscheinlich auch mit anderen Personen sicher kommunizieren; hierbei können zwei Schwierigkeiten auftreten:

* Sie wissen nicht immer, ob Ihr Gegenüber GnuPG benutzt oder überhaupt benutzen will.
* Selbst wenn Sie wissen, daß der andere GnuPG verwendet, könnten Sie Schwierigkeiten bei der Authentifizierung seines öffentlichen Schlüssels haben.

Das erste Problem rührt daher, daß viele Leute nicht öffentlich bekanntgeben, daß sie GnuPG benutzen. Am besten, Sie gehen mit gutem Beispiel voran und sorgen dafür, daß jeder Ihrer potentiellen Kommunikationspartner weiß, daß Sie GnuPG benutzen. Hierfür gibt es mehrere Möglichkeiten:

* Signieren Sie Nachrichten, die Sie an Ihre Korrespondenzpartner oder Mailinglisten verschicken, mit GnuPG.
* Veröffentlichen Sie Ihren öffentlichen Schlüssel auf Ihrer Website.
* Geben Sie Ihren öffentlichen Schlüssel auf einen Key-Server und veröffentlichen Sie die Schlüssel-ID in Ihrer E-Mail-Signatur oder auf Ihrer Visitenkarte.

Indem Sie Ihren Schlüssel bekannt geben, machen Sie es auch für andere akzeptabler, ihrerseits ihre Schlüssel bekannt zu geben. Außerdem erleichtern Sie es dadurch anderen, sicher mit Ihnen zu kommunizieren, da Sie die Initiative ergriffen und deutlich gezeigt haben, daß Sie GnuPG benutzen.

Die Authentisierung der öffentlichen Schlüssel ist schwieriger. Wenn Sie sich nicht persönlich von der Identität einer Person überzeugt haben, dann dürfen Sie deren Schlüssel auch **nicht** unterschreiben. In diesem Fall müssen Sie auf die Unterschriften von anderen vertrauen und hoffen, eine Kette von Unterschriften zu finden, die von dem betreffenden Schlüssel zurück zu Ihrem eigenen führt. Solch eine Kette kann nur zustande kommen, wenn Sie Ihren Schlüssel von anderen außerhalb Ihres anfänglichen **Web of Trust** haben unterschreiben lassen. Am einfachsten ist dies auf sogenannten Key-Signing-Partys zu erreichen: Das sind Zusammenkünfte, bei denen man sich gegenseitig authentifiziert und die öffentlichen Schlüssel unterzeichnet. Sollten Sie beispielsweise zu einer Konferenz gehen, halten Sie Ausschau nach einer Key-Signing-Party. Falls dort keine stattfindet, dann laden Sie doch einfach selbst zu einer ein. Auf jeden Fall sollten Sie aber Ihren GnuPG-Fingerabdruck immer bei sich haben (vielleicht auf Ihrer Visitenkarte) so daß Sie spontan mit anderen die Schlüssel tauschen können. Derjenige, dem Sie den Fingerabdruck gegeben haben, könnte dann, nachdem er Ihre Identität überprüft hat, bei der nächsten Gelegenheit Ihren öffentlichen Schlüssel unterschreiben.

Welchen Aufwand Sie betreiben, ist letztendlich Ihre Entscheidung und hängt allein von Ihren Sicherheitsbedürfnissen ab. Niemand ist verpflichtet, seinen Schlüssel öffentlich zu machen oder die Schlüssel anderer zu unterschreiben. Eine der Stärken von GnuPG ist die Flexibilität, mit der man die Benutzung den eigenen Ansprüchen anpassen kann. Sie werden jedoch feststellen, daß Sie Ihr **Web of Trust** ausbauen müssen, wenn sie GnuPG für Ihre sichere

Kommunikation einsetzen möchten.

8 Fußnoten

In diesem Abschnitt bezieht sich GnuPG sowohl auf die GnuPG-Implementierung von OpenPGP als auch auf andere Implementierungen wie das PGP-Produkt von NAI.