Sicher Emailen (PGP/GnuPG)

Burkhard Obergöker
Juli 07

Inhaltsverzeichnis

1 Warum Verschlüsselung?....3
2 Das Verfahren....4
2.1 Das Schlüsselpaar....4
2.2 Schlüssel-Signaturen....4
2.3 Email verschlüsseln....5
2.4 Email signieren....5
3 Benötigte Software....6
4 Eigenes Schlüsselpaar....7
5 Schlüssel-Signatur....9
6 Email verschlüsseln und signieren....10
6.1 Signieren....10
6.2 Verschlüsseln....10
7 Schlussbemerkungen....12

1 Warum Verschlüsselung?

Email hat sich in sehr vielen Bereichen als offizielles Kommunikationsmittel durchgesetzt. Kollegen bekommen Informationen, Nachbarn Urlaubsgrüße und Online-Shops Bestellungen über Email.

Nun ist aber mehr oder weniger bekannt, dass diese Email sehr viel Ähnlichkeit mit einer Postkarte hat: Jede Stelle, die sie bearbeitet oder weiterleitet, kann nicht nur den Inhalt einsehen, sondern auch verändern, ohne dass der Empfänger etwas davon merken würde. Auch wird der Sendende nicht dazu gezwungen, einen korrekten Absender anzubringen. Selbst wenn dieser völlig unsinnig wäre, würde die Karte zugestellt.

Das ist (normalerweise) noch nicht so dramatisch, wenn es sich um Urlaubsgrüße handelt, bei einer umfangreichen Bestellung oder einem Arbeitsauftrag wird das Ganze sehr sensibel. Im Bereich der „gelben“ Post verlässt man sich dann noch eher auf Briefumschläge und Rückmeldungen

Analog zu einem Briefumschlag kann der Inhalt einer Email verschlüsselt werden, so dass nur der Empfänger den Inhalt entziffern kann. Darüber hinaus kann aber auch noch sicher gestellt werden, dass der Inhalt unverfälscht ist und zusätzlich die Identität des Absenders gewährleistet wird.

Wie dieses erreicht werden kann, soll in diesem Kurs behandelt werden. Dabei wird bewusst nicht auf alle Fähigkeiten und Möglichkeiten eingegangen, um die Verwirrung nicht ganz so groß werden zu lassen.

2 Das Verfahren

Die Methode, die sich hinter den sicheren Emails verbirgt, beruht auf der sog. „asymmetrischen Verschlüsselung“. Dazu wird nicht ein Schlüssel zum ent- **und** verschlüsseln verwendet, sondern zwei, von denen einer **nur** zum verschlüsseln, der andere **nur** zum entschlüsseln verwendet wird.

2.1 Das Schlüsselpaar

Der Schlüssel zum verschlüsseln einer Nachricht ist der öffentliche Schlüssel (**public key**) und kann gefahrlos der gesamten Internet-Gemeinde bereit gestellt werden. Er muss sogar auf zentralen Servern (Keyserver) abgelegt werden, um benutzt werden zu können.

Der zweite Schlüssel ist geheim und wird als privater Schlüssel (**private key**) bezeichnet. Dieser darf nicht in die Öffentlichkeit gelangen, da nur dieser die verschlüsselten Nachrichten lesbar machen kann.

Der öffentliche Schlüssel wird auf einem zentralen Server (Keyserver) abgelegt, damit dieser weltweit verfügbar ist. Zur Verbesserung der Verfügbarkeit existieren mehrere dieser Keyserver, die sich untereinander abgleichen, so dass es ausreicht, den eigenen Schlüssel auf einen einzigen Server hochzuladen.

2.2 Schlüssel-Signaturen

Der Knackpunkt des Verfahrens ist jedoch die Frage, wie festgestellt werden kann, ob der Schlüssel auf dem Keyserver auch wirklich derjenige ist, der erwartet wird. Schließlich kann jeder einen öffentlichen Schlüssel ohne weitere Überprüfung der eigenen Identität hochladen. Für diesen Zweck wurde die Key-Signierung eingeführt. Dabei wird von einem anderen Key-Inhaber die Identität des Schlüssels bestätigt. Diese Signaturen werden an dem betreffenden Schlüssel vermerkt, so dass jeder, der sich den Schlüssel vom Keyserver herunterlädt, feststellen kann wie oft und von wem dieser Schlüssel bestätigt wurde. Dabei ist ein Schlüssel natürlich um so vertrauenswürdiger, je mehr Signaturen angehängt wurden. Auch der Ursprung der Signatur spielt eine Rolle: Eine Signatur von der Zeitschrift c't (Heise Verlag) ist sicherlich aussagekräftiger als die eines „Manfred Mustermann“ aus Pusemuckel.

Häufig ergibt sich in der Praxis ein Domino-Effekt: Wenn der Inhaber von Schlüssel X persönlich bekannt ist und dessen Signatur in Schlüssel Y auftaucht, dann wird dieser ebenfalls als vertrauenswürdig eingestuft.

Eine besondere Eigenschaft des Schlüssels ist der „Fingerprint“. Dabei handelt es sich quasi um die „Essenz“ des Schlüssels: Eine relativ kurze Folge von Buchstaben und Zahlen, die pro Schlüssel eindeutig und einmalig ist. Sinn eines solchen Fingerprints ist die Überprüfbarkeit. Wenn jemand den Fingerprint seines Schlüssels dem Empfänger persönlich übergibt, kann dieser leicht die Echtheit des entsprechenden Schlüssels überprüfen, indem er die Fingerprints miteinander vergleicht.

Um den eigenen Schlüssel in der Vertrauensstufe möglichst hoch zu bringen, lohnt es sich an „Keysigning Parties“ teilzunehmen. Dabei bringt jeder Teilnehmer den Fingerprint seines Schlüssels sowie zwei Amtliche Dokumente mit, die seine Identität bestätigen (meistens Personalausweis und Führerschein). Der Fingerprint wird jedem Teilnehmer ausgehändigt, so dass jeder Teilnehmer in der Lage ist, die Echtheit des Schlüssels mit seinem eigenen zu bestätigen. Auf diese Weise kommen relativ viele Signaturen mit geringem Aufwand zustande.

2.3 Email verschlüsseln

Jeder, der eine verschlüsselte Mail an den Eigentümer des privaten Schlüssels senden möchte, lädt den **öffentlichen Schlüssel** vom Keyserver und verschlüsselt damit die Email. Daraus entsteht ein scheinbares Wirrwarr von Zeichen, die niemand – auch nicht der Schreiber der Email – entschlüsseln kann. Lediglich der Eigentümer des privaten Schlüssels kann dieses Zeichen-Wirrwarr wieder in lesbare Information verwandeln. Daher reicht es nicht, nur den eigenen öffentlichen Schlüssel zu besitzen, für jeden Empfänger einer verschlüsselten Email muss ein solcher Schlüssel vorliegen.

2.4 Email signieren

Der Empfänger einer Email – egal, ob verschlüsselt oder nicht – kann im Normalfall nicht eindeutig feststellen, ob der Absender, der an der Email vermerkt ist, auch mit der realen Person identisch ist. Zu diesem Zweck wird eine Email signiert. Dabei wird mit dem **privaten Schlüssel** des Schreibers eine „Essenz“ der Email ermittelt und diese an die Email angehängt. Der Empfänger dieser Email kann nun mit dem öffentlichen Schlüssel des Absenders dessen Signatur überprüfen. Nur, wenn Absender, Datum und Inhalt der Email unverändert sind, bleibt die Signatur gültig. Anderenfalls wird die Signatur als ungültig bewertet. Bei sehr sensiblen Inhalten wird daher häufig die Email verschlüsselt **und** signiert.

3 Benötigte Software

Um die eigene Mail mit Verschlüsselung und Signatur schützen zu können, wird eine bestimmte Software benötigt. Ursprünglich wurde sie unter dem Namen „Pretty Good Privacy“ (PGP) entwickelt und als Open Source Software frei zugänglich gemacht. Leider entstand sie in den USA, deren Gesetze Verschlüsselungs-Software unter das Waffengesetz fallen lassen und somit einen Export verbieten. Da aber das Verfahren in der Mathematik ohnehin bekannt war, konnte diese Software unabhängig von dem ersten Produkt außerhalb der USA neu geschrieben werden. Dieses fand unter der Schirmherrschaft der FSF (Free Software Foundation) im Rahmen des GNU-Projektes statt. Daher war auch der Name „GNU Privacy Guard“ (GnuPG bzw. GPG) für die Software naheliegend. PGP und GPG sind -was die Verschlüsselung betrifft – völlig kompatibel, PGP kann aber kommerziell erworben werden und bietet zusätzlich Support und Tools. Beides kann allerdings auch mit der GPG erreicht werden.

Die reine GPG-Software ist ausschließlich zum Ent- und Verschlüsseln sowie zum Signieren gedacht. Sie ist rein Kommando-gesteuert und verzichtet bewusst auf den Ballast einer grafischen Benutzeroberfläche. Diese kann als separates Produkt die GPG-Software benutzen und wird in umfangreicher Weise angeboten.

In vielen Mail-Clients ist die Benutzung von GPG bereits eingebaut oder kann als Plugin nachgerüstet werden. Für Thunderbird bietet Enigmail eine umfangreiche Benutzungsumgebung, so dass Diese Kombination beispielhaft zeigen soll, wie Mail-Verschlüsselung genutzt werden kann.

Zunächst werden folgende Komponenten benötigt:

Produkt	Herkunft	Bedeutung
GnuPG	www.gpg.org	Zentrale Ver- und Entschlüsselungs-Software
Thunderbird	www.mozilla.org	Email-Clientsoftware
Enigmail	enigmail.mozdev.org	GPG-Plugin für Thunderbird

Sind alle Komponenten in dieser Reihenfolge installiert worden, kann mit den ersten Schritten begonnen werden.

4 Eigenes Schlüsselpaar

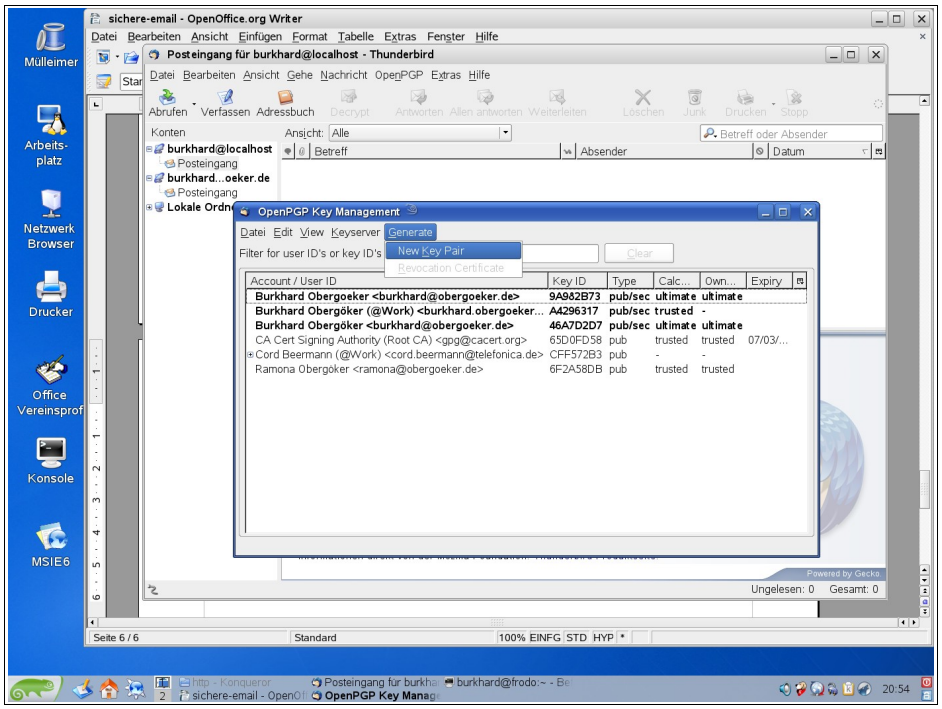
Um mit Verschlüsselung arbeiten zu können muss zunächst ein eigenes Schlüsselpaar erzeugt werden. Da dieser Vorgang üblicherweise einmalig ist, sollte er genau geplant werden. Besonders 2 Dinge sind von Relevanz:

a) Die Gültigkeit: Ein Schlüssel wird oft mit unbegrenzter Gültigkeit erzeugt. Er kann aber nicht von einem Keyserver gelöscht werden! Statt dessen wird im Bedarfsfall ein Widerruf-Schlüssel erzeugt, der den ursprünglichen Schlüssel quasi entkräftet. Da nicht alle Zielpersonen verlässlich erreicht werden, kann ein Missbrauch quasi unbegrenzt lange durchgeführt werden. Wird ein neuer Schlüssel erzeugt, müssen alle Signaturen neu eingeholt werden. Daher sollte die Gültigkeit begrenzt, die Dauer aber nicht zu klein gewählt werden.

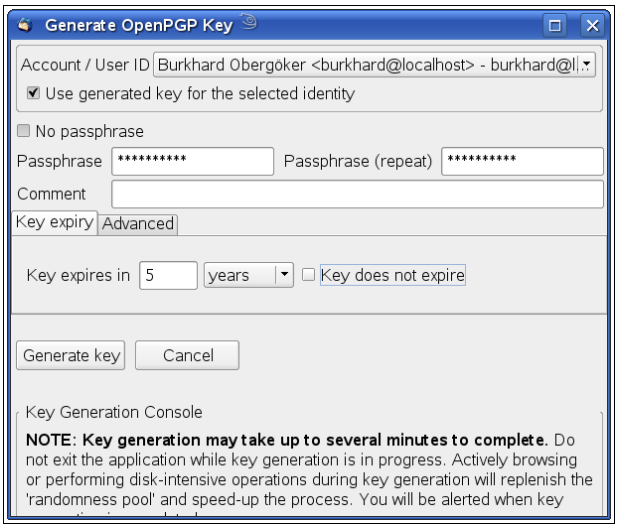
b) Sollte der private Schlüssel abgefangen werden, stellt das Passwort die letzte Hürde zum Missbrauch dar. Daher sollte ein Passwort gewählt werden, dass **nicht** aus „normalen“ Worten besteht, und mindestens 10 Zeichen lang sein. Auch sollte dieses Passwort nicht für weitere Zwecke (Email-Konto, Online-Banking, Internet-Zugang ...) verwendet werden, damit dieses nicht aus anderer Quelle bekannt werden kann.

Zusätzlich sollte noch einmal erwähnt werden, dass ein Schlüsselpaar an eine Email-Adresse gebunden ist. Sollte die Adresse ungültig werden, kann der Schlüssel nicht „übertragen“, sondern muss neu erzeugt werden.

In der Umgebung von Thunderbird wird die Generierung über den „OpenPGP“-Dialog erreicht. Unter „Key Management“ öffnet sich ein Dialog, in dem alle notwendigen Funktionen der Schlüsselverwaltung angeboten werden

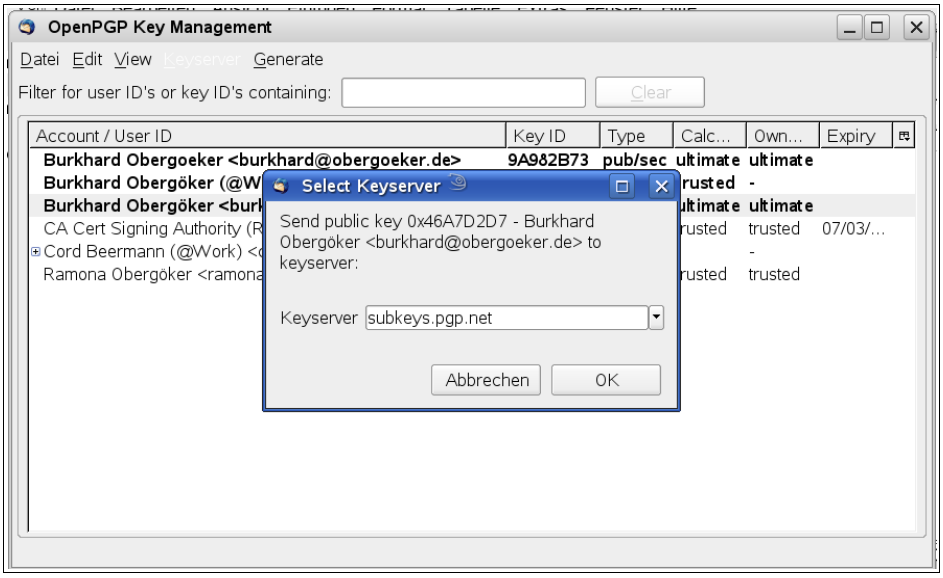


Dort kann im „Generate“- Menü auch ein neues Schlüsselpaar erzeugt werden. Werden mehrere Email-Konten in Thunderbird verwendet, sollte die gewünschte Email-Adresse ausgewählt werden, bevor das Schlüsselpaar erzeugt wird.



In dem folgenden Menü muss noch die Passwort-Phrase eingegeben werden, bevor der „Generate Key“-Knopf betätigt wird. Nach einiger Zeit wird der Erfolg der Generierung verkündet.

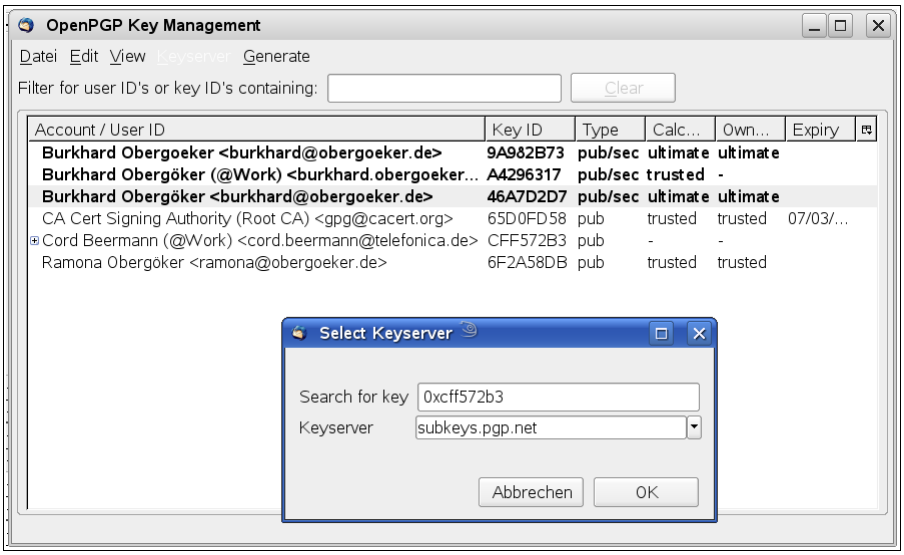
Nun muss noch der öffentliche Schlüssel auf einen Keyserver hochgeladen werden, um ihn bekannt zu machen. Dazu wird in dem OpenPGP-Dialog im Menü der Punkt „Keyserver -> Upload Public keys“ ausgewählt.



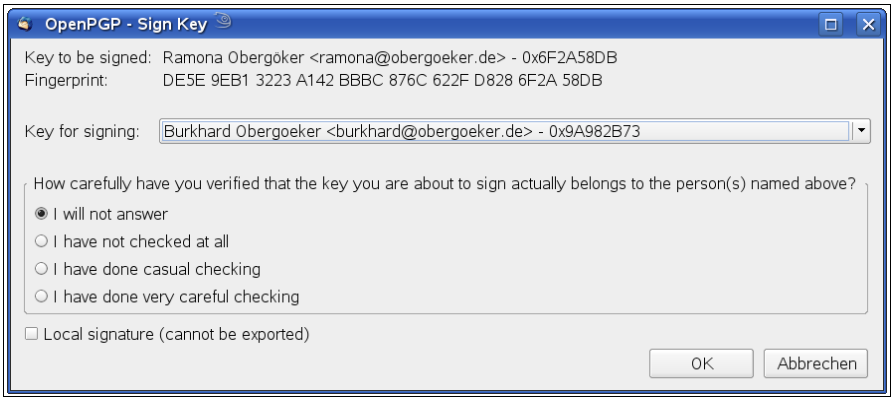
Nach der Angabe des gewünschten Servers wird der neue Schlüssel übertragen.

5 Schlüssel-Signatur

Um einen fremden Schlüssel zu signieren, muss dieser zunächst vom Keyserver herunter geladen werden. Dazu wird unter dem Menüpunkt „Keyserver -> Search for keys“ entweder die Email-Adresse oder die Schlüssel-Nummer (beginnend mit „0x“) eingegeben.



Wenn der gewünschte Schlüssel gefunden und in der Liste erschienen ist, reicht ein Rechtsklick auf diesen Eintrag, um den Punkt „Sign Key“ auszuwählen. Zur Kontrolle erscheinen Außer der Email-Adresse auch der Fingerprint und der Name des Schlüsselinhabers, um eine Kontrolle zu vereinfachen



Bevor die Signatur bestätigt wird, sollte der Grad der Kontrolle angegeben werden. Sie trägt zusätzlich zur Vertrauensstellung des Schlüssels bei. Wenn der Schlüsselinhaber mit Ausweis und Lichtbild überprüft wurde, ist der zweithöchste Grad („I have done casual checking“) der passende.

Die Signatur ist allerdings jetzt nur auf der lokalen Festplatte vermerkt. Um sie der Öffentlichkeit verfügbar zu machen, muss dieser Schlüssel wieder auf einen Keyserver geladen werden. Das funktioniert genau wie das Hochladen des eigenen Schlüssels (s. (4)). Die Software des Keyservers vermeidet dabei automatisch Kollisionen, so dass niemand die Einträge eines Anderen überschreiben oder gar löschen kann.

6 Email verschlüsseln und signieren

Nach diesen ganzen Vorarbeiten ist es jetzt endlich möglich, eine Email zu verschlüsseln und zu signieren. Dabei muss beachtet werden, dass unterschiedliche Schlüssel für die beiden Zwecke benötigt werden.

6.1 Signieren

Das einfachere Verfahren ist dabei die Signatur einer Email. Bitte eine Email-Signatur nicht verwechseln mit einer Schlüssel-Signatur. Beides klingt zwar ähnlich, dahinter verbergen sich jedoch völlig unterschiedliche Vorgänge mit verschiedenen Zielen.

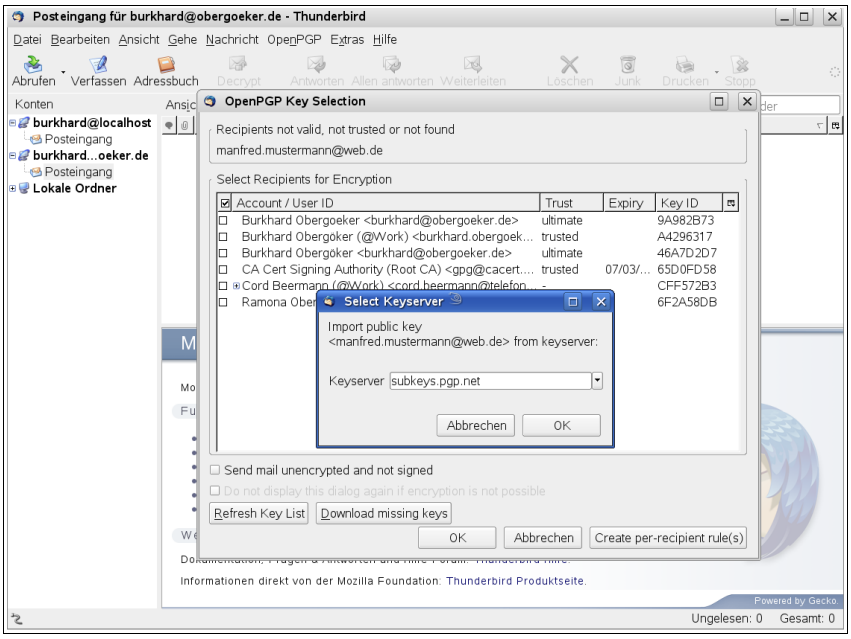
Die Signatur wird immer mit dem eigenen privaten Schlüssel vorgenommen, und bedarf daher keinerlei Vorarbeiten. Eeine Email wird wie gewohnt geschrieben, lediglich vor dem Versandt wird über das Menü (OpenPGP -> Sign Message) festgelegt, dass die Email verschlüsselt werden soll.

Wenn der Versandt initiiert wird, sorgt Thunderbird selbstständig für die Verschlüsselung der gesamten Mail. Sollten Anhänge angefügt worden sein, können diese auch in die Verschlüsselung einbezogen werden, was vor allem dann sinnvoll ist, wenn es sich um Dokumente wie Auftragsbestätigungen, Bestellungen und ähnlichem handelt.

Sofern der Empfänger auch mit einem PGP/GPG-fähigen Emil-Client ausgestattet ist, wird dieser den Benutzer bei Empfang darauf hinweisen, dass die Email verschlüsselt ist. Zur Überprüfung wird aber der öffentliche Schlüssel des Absenders benötigt, so dass dieser zunächst von einem Keyserver herunter geladen werden muss, sollte er nicht bereits in der eigenen Liste enthalten sein. Thunderbird übernimmt diese Aufgabe aber fast vollautomatisch, so dass lediglich das Ergebnis der Überprüfung betrachtet werden muss.

6.2 Verschlüsseln

Etwas mehr Vorarbeit ist bei der Verschlüsselung der Email notwendig, da hier **vor** dem Versandt der öffentliche Schlüssel des Empfängers bekannt sein muss. Wird die Email geschrieben, bietet wiederum das OpenPGP-Menü die Verschlüsselung an.



Erst, wenn der „Senden“-Knopf betätigt wird, erscheint ein Dialogfenster, in dem der oder die fehlenden Schlüssel nachgeladen werden können. Findet dieses erfolgreich statt, wird die Email gesendet, anderenfalls wird eine Fehlermeldung ausgegeben und der Versandt abgebrochen. Es wird also nicht „versehentlich“ unverschlüsselt gesendet.

7 Schlussbemerkungen

Es bleibt also zu bemerken, dass die Verwendung von Email-Verschlüsselung und -Signatur. nach einiger Gewöhnung wesentlich weniger aufwändig ist, als es zunächst den Anschein hat. Die Güte dieser Verfahren ist jedoch abhängig von der Aktualität und Vollständigkeit der Schlüssel-Liste und der Sicherheit der eigenen privaten Schlüsseln. Es lohnt sich darüber hinaus, an möglichst vielen Keysingning-Parties teilzunehmen, nicht nur um den eigenen Schlüssel signieren zu lassen, sondern auch um möglichst viele Personen „hinter“ den Schlüsseln persönlich kennen zu lernen. Auch sollte es zur guten Gewohnheit werden, die Key-Liste häufig, möglichst täglich zu aktualisieren, indem die Schlüsseleinträge vom Keyserver geladen werden. Dadurch werden abgelaufene und ungültige Schlüssel schnell erkannt und deren Verwendung vermieden.