Kryptographie für alle

Bernd Weber

6. August 2008

Inhaltsverzeichnis

Einleitung

Zunächst einmal: Was ist Kryptographie? Kryptos, altgriechisch, ist »das Verborgene«. »Graphein« heißt schreiben. Wörtlich heißt es in etwa »verborgen schreiben«. In verständlichem Deutsch handelt es sich um die Kunst des Ver- und Entschlüsselns von Nachrichten. Warum müssen wir uns damit beschäftigen? Ist das nicht etwas für Geheimdienste? Wir bewegen uns im Internet. Umverschlüsselte E-Mails zu verschicken ist vergleichbar dem verschicken von Postkarten, die jeder lesen kann. Wir können nicht nachprüfen, was zwischen Versand und Empfang von Nachrichten passiert. Zum einen kann ein begehrlicher Staat, der seinen Bürgern immer weniger traut, den E-Mail-Verkehr lückenlos überwachen wollen. Im harmloseren Falle könnte ein gelangweilter Webmaster (diese sind im allgemeinen selten gelangweilt, sondern meistens im Stress) ein Vergnügen daran haben, fremde Post zu lesen. Firmen können ein Interesse daran haben, Profile potentieller Kunden zu erstellen und Betreiber von Servern können Daten von Usern verkaufen, auch wenn das nicht legal ist – wissen wirs? Wie auch immer – Gründe, E-Mails zu verschlüsseln gibt es reichlich.

1 Gibt es den sicheren Schlüssel?

Antwort von Radio Eriwan: Im Prinzip ja, aber dann müsste der Schüssel genauso lang sein, wie der zu verschlüsselnde Text. Die Wissenschaft, die zur Kryptographie gehört, ist die Kryptologie, ein Teilgebiet der Mathematik. Es lässt sich streng mathematisch beweisen, dass es einen absolut sicheren Schlüssel geben könnte. Ein darauf beruhendes Verschlüsselungsverfahren wäre kaum praktikabel. In der Praxis reicht es jedoch, wenn der Zeitaufwand mit herkömmlichen Codeknackverfahren und Comptern unvertretbar hoch würde. Der mit openPGP hergestellte Code ist in diesem Sinne abzählbar sicher. Das heißt, dass die ganze Rechenkapazität dieses Planeten, immer den heutigen Stand angenommen, noch mit der Entschlüsselung einer DIN-A-4-Seite beschäftigt wäre, wenn die zu einem rote Riesen aufgeblähte Sonne dabei wäre, die Erde zu einer Terrakottakugel zu schmoren.

2 Wie funktionert OpenPGP?

OpenPGP funktioniert nach dem zwei-Schlüssel-Verfahren. Ein Schlüssel, der öffentliche Schlüssel wird zum Verschlüsseln der Nachricht, der andere, der private oder geheime Schlüssel wird zum Entschlüsseln verwendet. Der Vorteil liegt auf der Hand. Die Verständigung mit dem Kommunikationspartner über den eingesetzten Schlüssel kann völlig offen bewerkstelligt werden. Die Schlüssel müssen nicht über verschlungene, geheime Pfade ausgetauscht werden. Eine einmal verschlüsselte Nachricht kann nur mit dem Komplementärschlüssel, der auf dem Rechner des Empfängers bleibt, wieder entschlüsselt werden. Kann ich OpenPGP auch unter Windows nutzen? Ja. Obwohl der Verfasser dieser Zeilen normalerweise mit LINUX arbeitet, sind die folgenden Anweisungen auf den Windows-Nutzer abgestimmt.

3 Welche Programm benötige ich?

- pgp4win kann unter `ftp://ftp.gpg4win.org/gpg4win-1.1.3.exe` heruntergeladen werden.
- Thunderbird kann unter `http://downloads.mozilla.org/?product=firefox-2.0.0.8&os=win&lang=de` heruntergeladen werden.
- Das Enigmail-Add-On zu Thunderbird

Diese Programme werden als setup-exe-Programme auf dem Rechner in einem Verzeichnis Ihrer Wahl gespeichert. Ich denke, zur Programminstallation unter Windows brauche ich nicht viel zu erzählen. Man klickt die Setup.exe-Datei an und akzeptiert eine Lizenzvereinbarung. Normalerweise kann man dann einfach weiter klicken, da Otto-Normalnutzer im allgemeinen mit der Standardinstallation zufrieden sein kann. Um pgp4win brauchen wir uns erst einmal überhaupt nicht zu kümmern. Es ist jetzt einfach

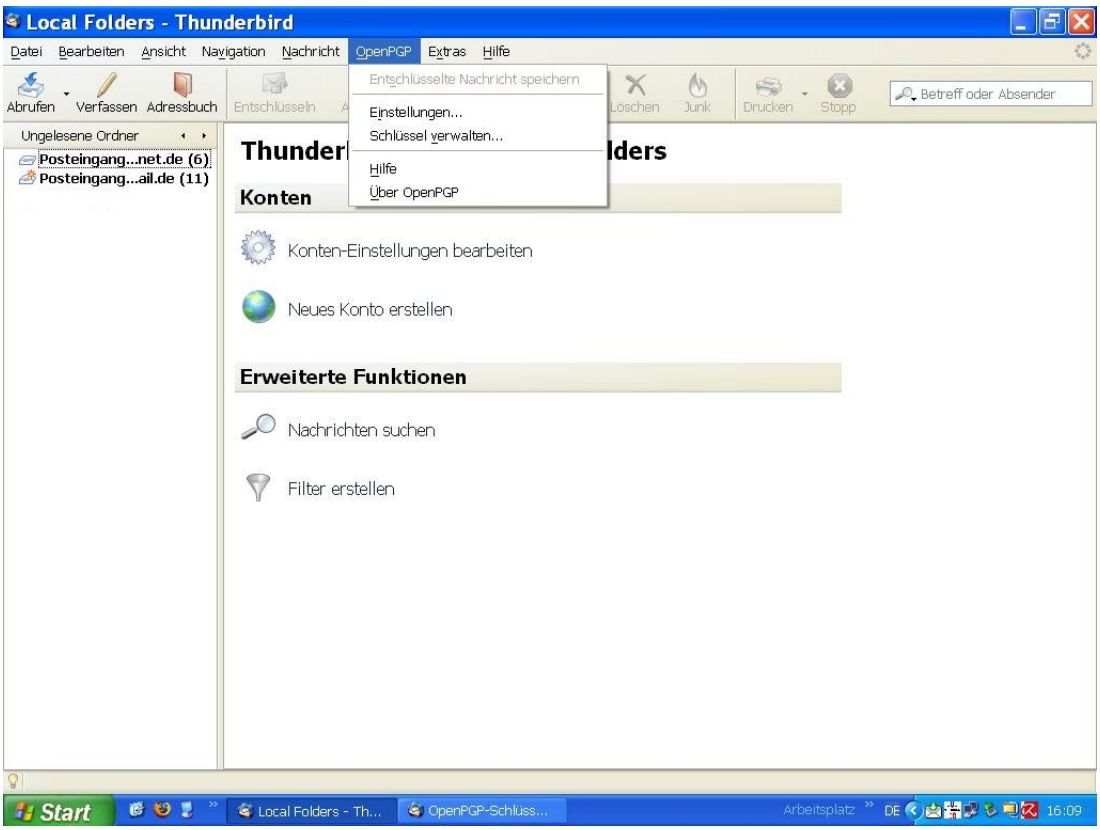
auf dem Rechner installiert. Die Installation von Enigmail setzt die vorangehende Installation von Thunderbird voraus. Dieser wenden wir uns deshalb im nächsten Abschnitt zu.

4 Einrichtung von Thunderbird

Zuerst rufen wir Thunderbird auf. Wir werden jetzt aufgefordert, einen E-Mail-Account anzulegen (sollte nicht schon einer aus einer früheren Installation existieren). Noch einmal zur Erinnerung: Wir können unsere E-Mails unter verschiedenen Identitäten verfassen. Zu einer Identität gehört eine Bezeichnung – nur zur Erinnerung für uns (wir können sie auch haumichblau nennen), verschiedene Angaben, die in der E-Mail auftauchen können, verschiedene Verschlüsselungseigenschaften und zu guterletzt Posteingangs- und Postausgangsserver. Posteingangsserver beginnen meistens mit pop oder pop3 bzw. imap (Beispielsweise imap.freent.de). Postausgangsserver beginnen meistens mit smtp, heißen oft aber auch anders (mx.freenet.de, mail.imail.de, smtp.web.de). Für Benutzer von web.de heißt der Ausgangsserver immer smtp.web.de. Wir müssen noch Benutzernamen und gegebenenfalls Passwort eingeben. Das Passwort wird spätestens dann abgefragt, wenn wir Post empfangen oder verschicken wollen. Wenn wir unsere Postfächer später einrichten wollen, können wir den Einrichtungsdialog hier auch abbrechen. Wir können später darauf zurückkommen, wenn wir im Menü: Bearbeiten -> Konten wählen. Wer schon ein E-Mail-Konto unter Outlook eingerichtet hat, wird auch hier keine Probleme haben. Die Dialoge sind ähnlich. Nach Einrichten des E-Mail-Kontos wenden wir uns der Installation von Enigmail zu. Dazu gehen wir im Menu-Bar auf Extras -> Erweiterungen. In dem Fenster das sich öffnet klicken wir den Link: Erweiterungen herunterladen (oder Falls wir die Englische Version haben download Add-Ons) an. Nun öffnet sich der Standardbrowser mit der Add-On-Seite von Firefox. Links wählen wir Thunderbird aus. Nun müssen wir noch Enigmail suchen. Für die Ungeduldigen ist hier schon mal der Download-Link: `https://addons.mozilla.org/de/thunderbird/downloads/file/20480/enigmail-0.95.5-tb+sm.xpi` Dieser kann sich jedoch schon mal ändern, weshalb ich oben dieses Prozedere angegeben habe. Auch wenn es der Browser anbieten sollte, falls Firefox benutzt wird, sollte man dies auf keinen Fall tun, da es sich ja um eine Erweiterung für den Thunderbird handelt. Wir speichern die .xpi-Datei also zuerst mal auf der Festplatte. Anschließend öffnen wir den Thunderbird, wählen im Menü wieder Extras und dann Installieren aus. Im sich öffnenden Datei-Dialog suchen wir jetzt die xpi-Datei heraus, die wir gerade heruntergeladen haben. Enigmail wird jetzt installiert. Wir beenden Thunderbird.

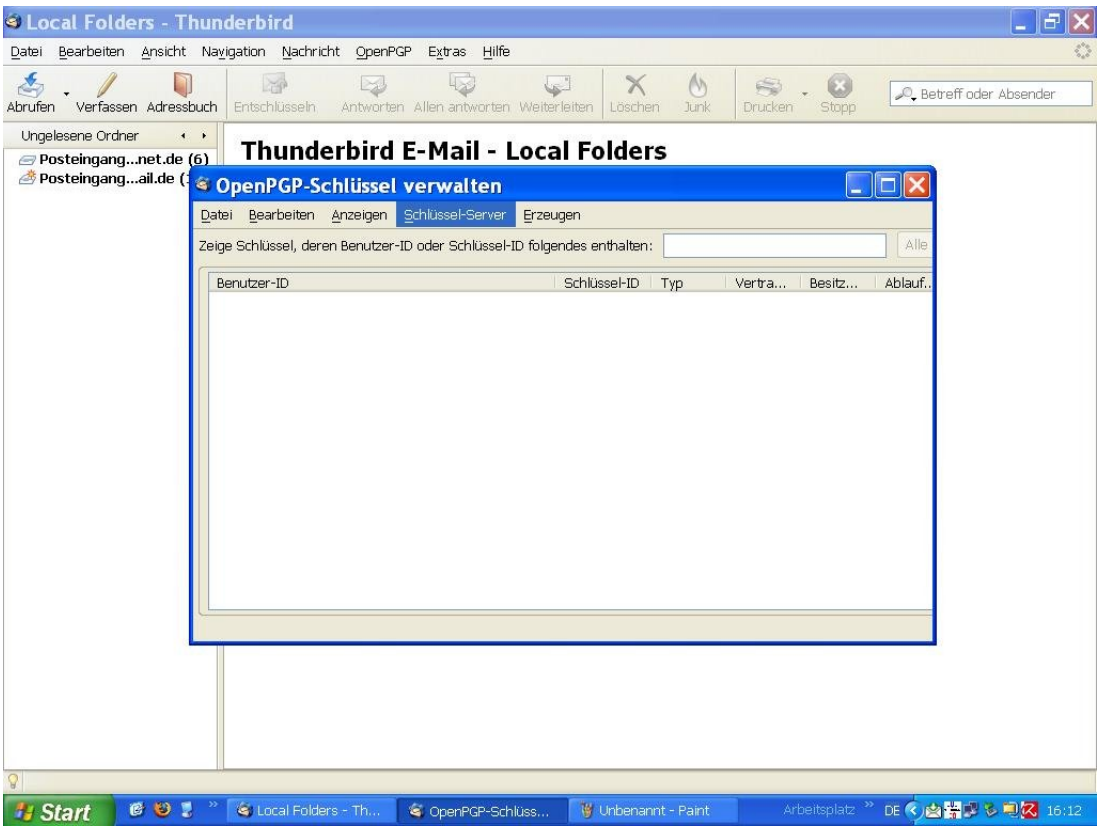
5 Schlüssel verwalten mit Enigmail

Wir starten jetzt Thunderbird neu. Jetzt sollte in der Menü-Leiste ein neuer Eintrag hinzugekommen sein: openPGP. Screenshot 1 zeigt das Dropdown-Menü von openPGP.



Screenshot 1: Ausgeklapptes PGP-Drop-Down-Menü

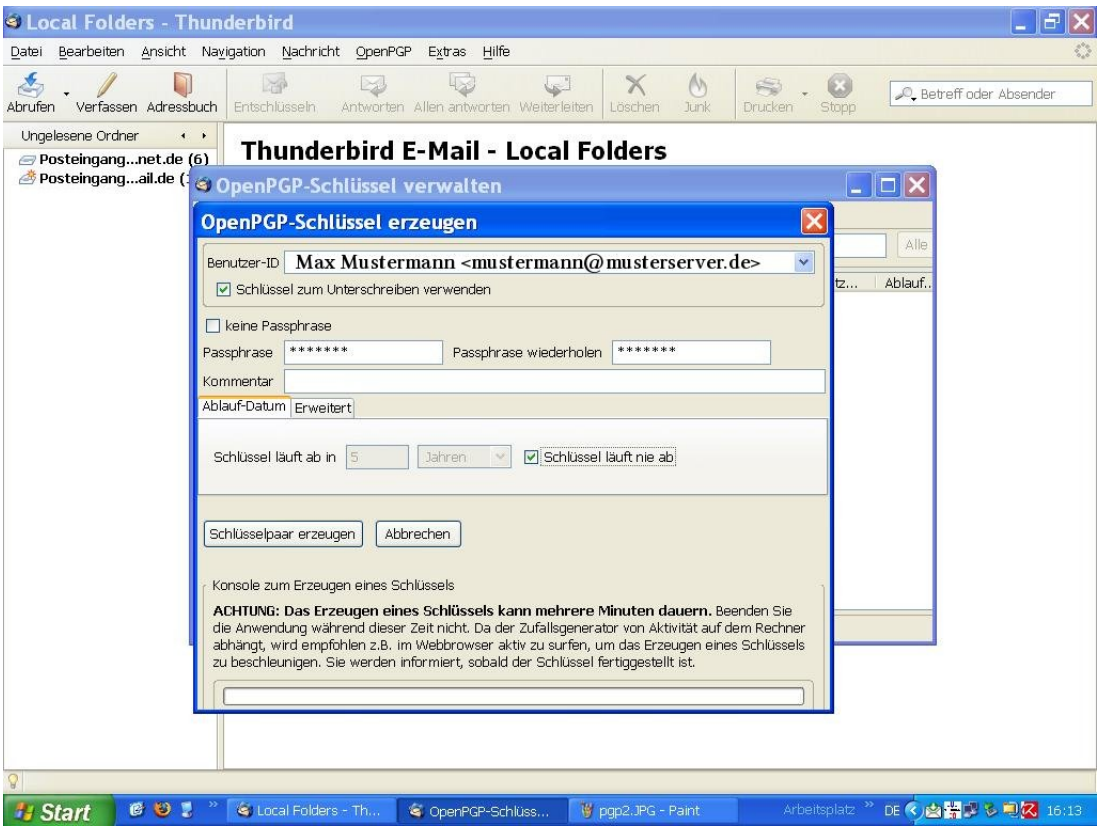
Wir wählen SCHLÜSSEL VERWALTEN.... Screenshot 2 zeigt den Schlüsselverwaltungsdialog. Für uns haben wir noch keinen Schlüssel festgelegt.



Screenshot 2: Schlüsselverwaltungsdialog 1

Wir müssen also erst einmal ein Schlüsselpaar generieren. Ein Schlüssel davon, der private, verbleibt ausschließlich bei uns auf dem Rechner und ist durch eine Passphrase (dazu später) geschützt. Der andere Schlüssel, der öffentliche, dient unseren Kommunikationspartnern dazu, Nachrichten an uns zu verschlüsseln. Wir ignorieren in diesem Dialog also erst mal alle anderen Menüpunkte und wählen hier ERZEUGEN (oder GENERATE) aus.

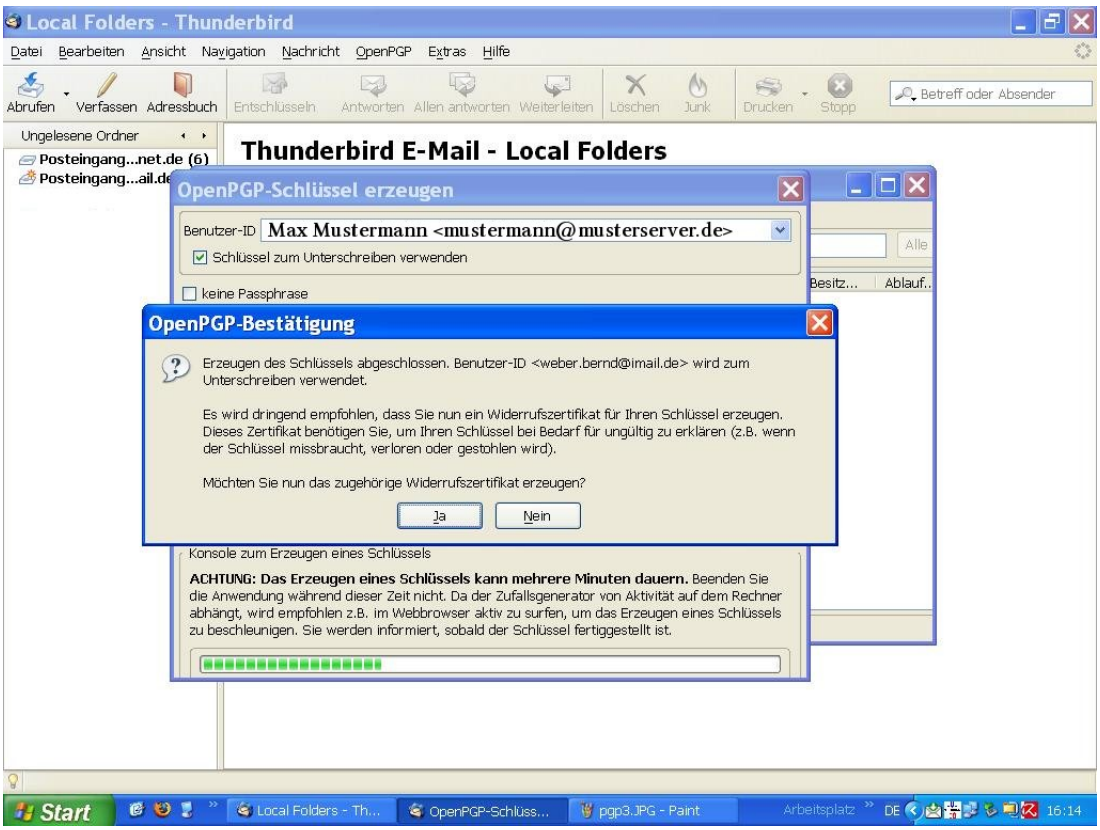
Als nächstes werden wir aufgefordert, eine Passphrase festzulegen. Es heißt hier nicht Passwort, sondern Passphrase, manchmal auch Mantra genannt, weil Sie durchaus länger und nicht so einfach wie ein Passwort sein sollte, um größere Sicherheit zu gewährleisten. Diesen Dialog zeigt uns Abbildung 3.



Screenshot 3: Schlüsselverwaltungsdialog 2

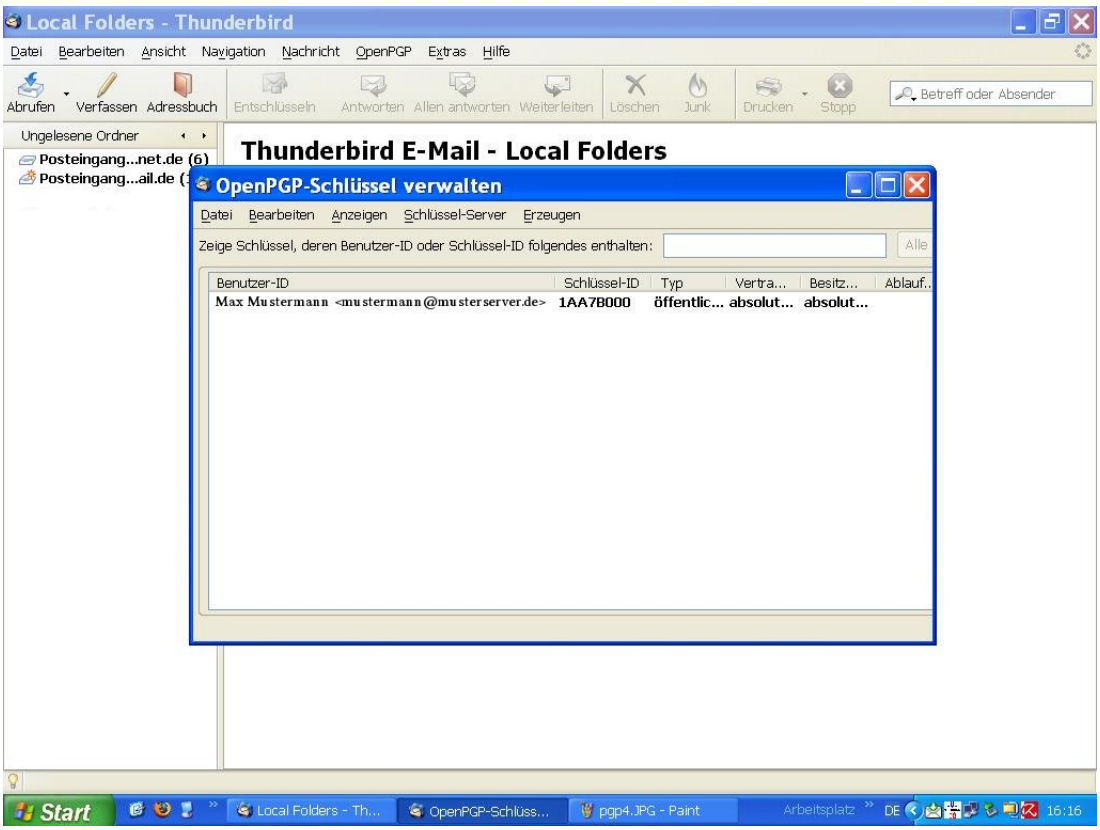
Für Demonstrationszwecke ist in die Felder schon mal was eingetippt. Die hier gezeigte Passphrase ist im wirklichen Leben allerdings etwas kurz geraten. Die Passphrase sollte aus einer Kombination von alphanumerischen Zeichen und Sonderzeichen bestehen – z.B. A,b,C,@,1,4, – Leerzeichen sind nicht geeignet. Wir müssen diese Passphrase ein zweites Mal eingeben, um sicher zu stellen, dass wir uns beim ersten Mal nicht vertippt haben. Jetzt müssen wir noch SCHLÜSSELPAAR ERZEUGEN anklicken und warten erst mal ab, denn dieser Vorgang kann ein paar Minuten dauern.

Wenn der Vorgang abgeschlossen ist, öffnet sich ein neuer Dialog, in dem uns nahe gelegt wird, ein Widerrufszertifikat zu erstellen. Das tun wir denn auch. Dieses Zertifikat kann gegebenenfalls über den Import-Dialog importiert werden und sperrt den aktuellen privaten Schlüssel, falls dieser kompromittiert ist (Abbildung 4).



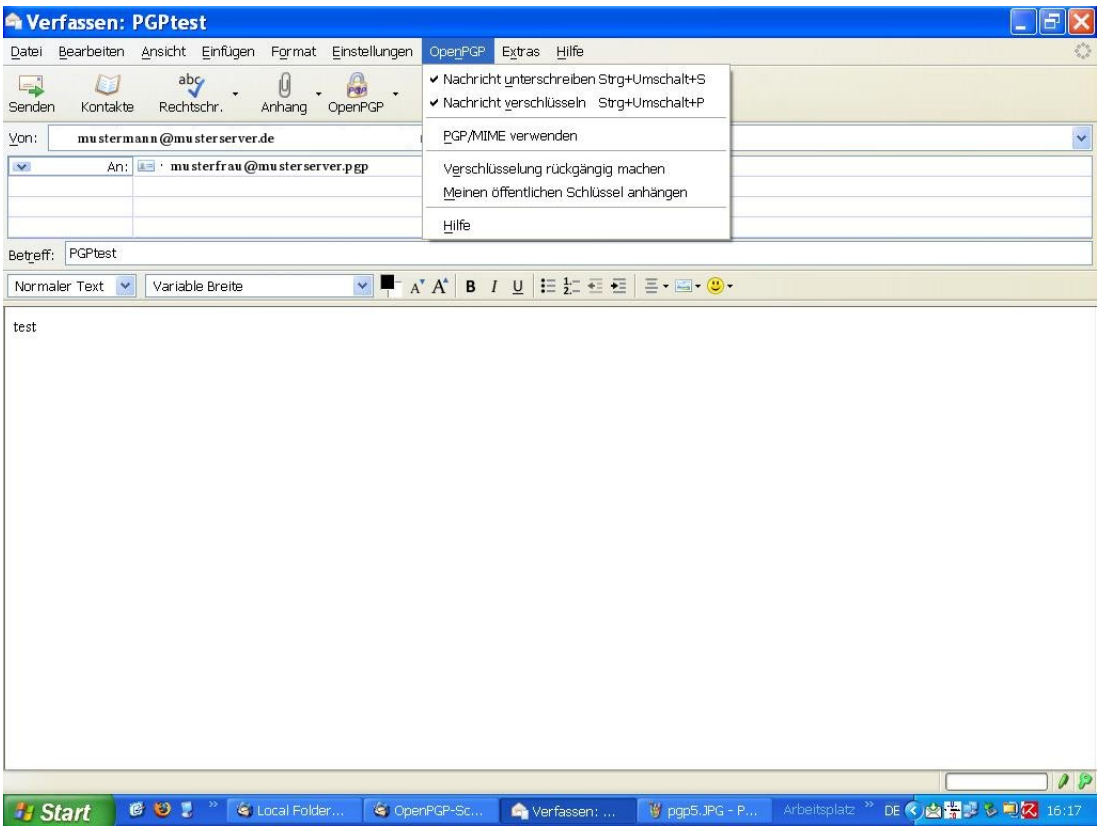
Screenshot 4: Die Passphrase

Wir können nun anderen unseren öffentlichen Schlüssel zur Verfügung stellen, indem wir ihn zum Beispiel in einer E-Mail, die natürlich noch unverschlüsselt ist, anhängen (Abbildung 5).



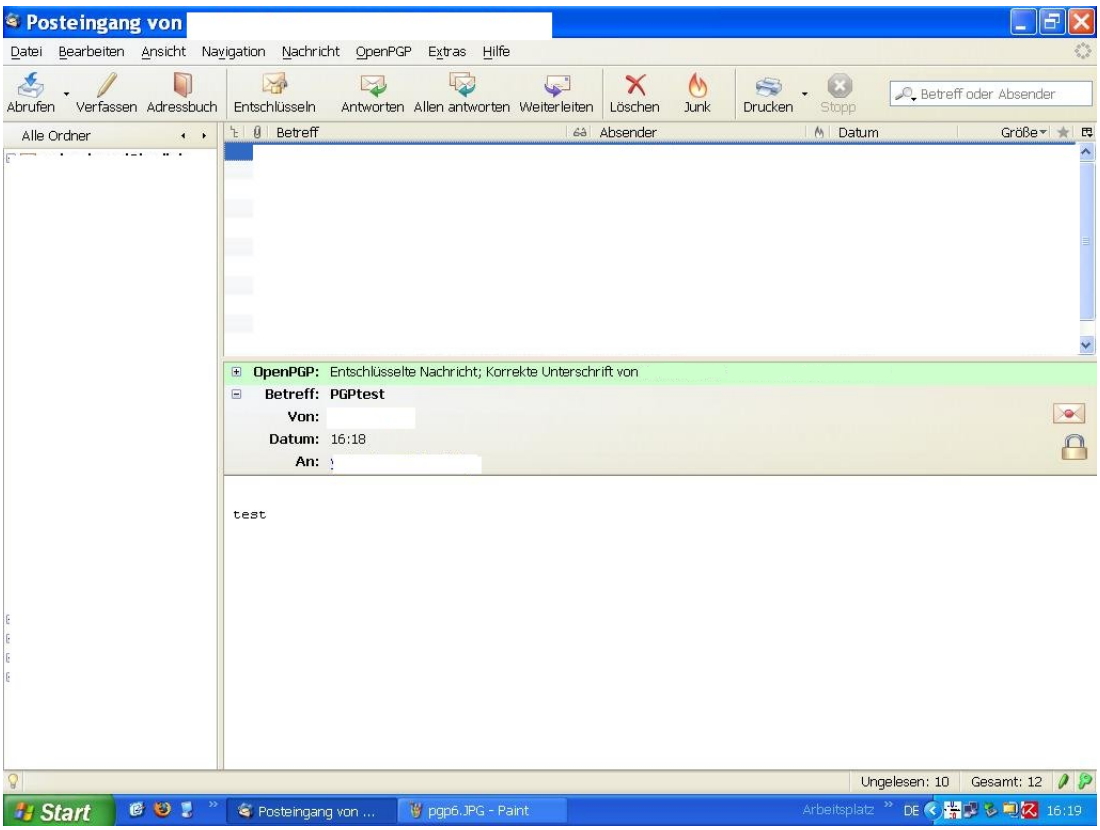
Screenshot 5: Das Widerrufszertifikat

Dazu wählen wir im Drop-Down-Menü: "Meinen öffentlichen Schlüssel anhängen". Wenn wir uns selber zu Testzwecken eine verschlüsselte Mail schicken wollen, können wir das sofort tun, wenn wir im Drop-Down-Menü "Nachricht verschlüsselnäuswählen. Wir können Nachrichten auch mit unserem Schlüssel signieren (unterschreiben), damit unser Kommunikationspartner die Authentizität der Nachricht überprüfen kann. Dazu werden wir aufgefordert, unsere Passphrase einzugeben.



Screenshot 6: Verschlüsseln von Nachrichten

Die Nachricht wird entschlüsselt. Thunderbird erkennt automatisch, dass es sich um eine verschlüsselte Nachricht handelt und fordert uns auf, die Passphrase einzugeben. Ist diese korrekt, wird die Nachricht sofort entschlüsselt und wie in Abbildung 7 zu sehen, angezeigt.



Screenshot 7: Verschlüsseln von Nachrichten

6 Weiterführende Informationen – Ausblick

Nach der Standardinstallation von gpg4win ist auch das Elektronische Handbuch dazu vorhanden. Wenn wir unter dem START-Menü von Windows nach gpg4win suchen, werden wir fündig. Diese Anleitung soll nur einen schnellen Einstieg vermitteln. Angeblich soll auch ein Plugin zu gpg4win für Outlook-Express existieren. Darüber gibt auch das Handbuch weitere Auskunft. Ich persönlich empfehle trotzdem Thunderbird, weil die meisten Angriffe, seien es Phishing- oder Trojanerattacken, sich auf Outlook kaprizieren und Thunderbird selber über weitergehende Sicherheitsmechanismen verfügt.