

Seminar 13.11.2008

Der sichere elektronische Briefverkehr
oder
einfach verschlüsselte E-Mails

Thomas Maurer
Diplomkaufmann Steuerberater

Am Weidengraben 11
21481 Lauenburg

Telefon: 04153/582358

Telefax: 04153/582356

e-mail: maurer@maurer-stb.de

Was ist eine E-Mail.....	3
E-Mail ist wie eine Postkarte	3
Wie kann ich mich vor den Blicken andere schützen???	4
Wie funktioniert das System.....	5
Wie kann ich das System installieren und nutzen.	7
Erstes wird ein Verschlüsselungsprogramm benötigt:	7
Zweitens benötigen Sie ein E-Mail Programm	9
Schlüsselerstellung	14
E-Mail Programm	15
Schlüsselversendung.....	16
Empfangen von öffentlichen Schlüssel	17
Versenden von E-Mail	18

Was ist eine E-Mail

laut Wikipedia, der freien Enzyklopädie

Die (auch das) E-Mail [ˈiːmeɪl] (kurz Mail; von englisch: „electronic mail“; zu deutsch: „die elektronische Post“ oder „der elektronische Brief“) bezeichnet eine auf elektronischem Weg in Computernetzwerken übertragene, briefartige Nachricht. Eindeutschungen wie „E-Brief“, „E-Post“ oder „Netzbrief“ sind weniger verbreitet.

E-Mail wird – noch vor dem World Wide Web – als wichtigster und meistgenutzter Dienst des Internets angesehen. Allerdings ist seit ca. 2002 über die Hälfte des weltweiten E-Mail-Aufkommens auf Spam zurückzuführen

E-Mail ist wie eine Postkarte

E-mail sind überhaupt nicht sicher, sie sind wie eine Postkarte.....

...warum sind E-Mail wie eine Postkarte? Ganz einfach, es ist eine offene Textdatei, die unterwegs jeder lesen kann. Und das muss ja nicht unbedingt sein, auch wenn es nicht die allergeheimsten Inhalte sind, die man sich mitzuteilen hat. Es geht einfach prinzipiell niemanden etwas an. Meine konventionellen Briefe klebe ich ja auch zu.

Um so erstaunlicher finde ich es, wie sorglos viele Leute persönlichste Dinge per E-Mail schreiben – ohne sich darüber im Klaren zu sein, dass eine E-Mail nicht nur gelesen, sondern sogar problemlos automatisch kopiert und archiviert werden kann.

In unserm Bereich sind die Daten die wir versenden sehr intim, es handelt sich um Ihre wirtschaftlichen und persönlichen Verhältnisse.

Überall wird der Datenschutz hoch gesetzt und Wir/Sie nutzen das Internet und damit auch das Versenden von e-mail, ohne Scham.

Es ist oft so, dass komplette Bilanzen und BWA's ohne Sicherung und Schutz gegenüber ungebeten Lesern weiter geleitet werden.

Wenn Ihre Post vertauscht und Ihre Belege und BWA bei Meier ankommen, ist das eine Katastrophe. So etwas darf nicht passieren, das Fremde Ihre Sachen lesen können, doch eine Bilanz oder Steuererklärung wird ohne weitere Fragen an die Bank gemailt.

Mit diesem Seminar möchte ich Ihre Privatsphäre retten.

Mit Hilfe von Verschlüsselung ist Ihre E-Mail vor fremden Lesern geschützt. Es geht um Ihre Privatsphäre.

Wie kann ich mich vor den Blicken andere schützen???

Zu diesem Zweck gibt's Verschlüsselungs-Software wie z.B. „**Pretty Good Privacy**“ (**PGP**). Der Name „Ziemlich gute Vertraulichkeit“ ist noch untertrieben; PGP ist praktisch nicht zu knacken – so viel Zeit und Geld, wie dafür nötig wäre, investiert jedenfalls keiner, um Ihre Post zu lesen! (In den USA fiel PGP daher sogar für lange Zeit unter die Waffenexportgesetze. Aber das nur am Rande.)

Eine weitere Möglichkeit ist die Open-Source-Version GnuPG, diese öffentlich“ und dezentral gepflegten Software sind vertrauenswürdiger als eine kommerzielle PGP Software.

Was Sie mit PGP anfangen können

Der Sinn von PGP besteht, wie gesagt, darin, Ihre Privatsphäre zu schützen – Ihre elektronische Korrespondenz soll privat bleiben, und Texte bzw. Dateien sollen vor Manipulation geschützt werden. PGP bietet Ihnen dafür im Wesentlichen zwei Funktionen:

Verschlüsseln von Texten (oder kompletten Dateien), die nur ein ganz bestimmter Personenkreis lesen können soll – zum Beispiel ein Briefempfänger und Sie selbst. Für alle anderen Leute ist das völlig wirrer Zeichensalat. Ihre Korrespondenz ist auf diese Weise sicherer vor neugierigen Augen geschützt als in Briefumschlägen, die ja eigentlich leicht zu öffnen sind.

Unterschreiben von Texten (oder kompletten Dateien), die zwar jeder lesen darf, die aber nicht verändert werden dürfen oder sollen. Das geschieht so, dass aus Ihrem Text und Ihrem PGP-Schlüssel eine „Quersumme“ errechnet und an den Text angehängt wird. Jeder, der auch PGP und Ihrem Schlüssel hat, kann prüfen, ob die elektronische Unterschrift noch mit dem Text übereinstimmt

PGP Verschlüsselt mit einem Schlüssel.





Diesen erhalten Sie von der Zentrale-Schlüsselverwaltung.



Bei der Verschlüsselung mit einem Schlüssel werden alle Informationen in der E-Mail mit einem besonderen System verschlüsselt, dass nur mit dem richtigen Schlüssel wieder lesbar gemacht werden kann.

Wie funktioniert das System

Im Gegensatz zu herkömmlicher Verschlüsselungstechnik werden **keine** "abhörsicheren Kanäle" gebraucht, durch die zwischen Sender und Empfänger die Schlüssel ausgetauscht werden. Außerdem muss man die öffentlichen Schlüssel nicht verstecken, was zusätzlich die Sicherheit des Verfahrens erhöht.

Es wird über einen Schlüsselservers ein Schlüsselpaar erzeugt. Das Erzeugen der Schlüssel werde ich später bei der Installation zeigen.

Wenn Sie sich PGP besorgt und installiert haben, erzeugen Sie sich erst einmal ein Schlüsselpaar  , bestehend aus dem **öffentlichen Schlüssel**  (**Public-Key**) und dem **privaten bzw. geheimen Schlüssel**  (**Secret- oder Private-Key**).

Der private Schlüssel  wird nicht herausgegeben und muss sorgsam gehütet werden. Jeder, der Ihnen eine mit PGP verschlüsselte Nachricht zukommen lassen will, benötigt hierfür Ihren öffentlichen Schlüssel .

Man spricht daher auch von einer **Public-Key-Verschlüsselung**. Die Nachricht wird vom Absender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und an ihn geschickt. Nur der Empfänger kann die für ihn bestimmte Nachricht mit seinem privaten Schlüssel entschlüsseln.

Der **öffentliche Schlüssel** ist für alle Aktionen zuständig, die **jedermann** machen darf:

- Nachrichten an Sie verschlüsseln
- Ihre Pop-Unterschriften prüfen

Der **private Schlüssel** ist für alle Aktionen zuständig, die **nur Sie** machen können:

- An Sie gerichtete Nachrichten entschlüsseln
- Nachrichten, Dateien oder andere Schlüssel unterschreiben

Ein **private Schlüssel** und sein **öffentlichen Schlüssel** bilden ein Paar wie Schlüssel und Schloss:

Ein privater Schlüssel kann immer nur die Nachrichten entschlüsseln, die auch mit dem dazu gehörenden privaten Schlüssel verschlüsselt wurden. Wenn ein privater Schlüssel verloren geht, ist der dazugehörige private Schlüssel nicht mehr zu gebrauchen. Und umgekehrt.

Ihren **öffentlichen Schlüssel** geben Sie an alle Leute weiter, mit denen Sie in Verbindung stehen. Mit diesem Schlüssel können die Nachricht nur **verschlüsseln**, aber nicht wieder **entschlüsseln** werden.

Umgekehrt besorgen Sie sich die **öffentlichen Schlüssel** aller Leute, denen Sie verschlüsselte Nachrichten schicken wollen.

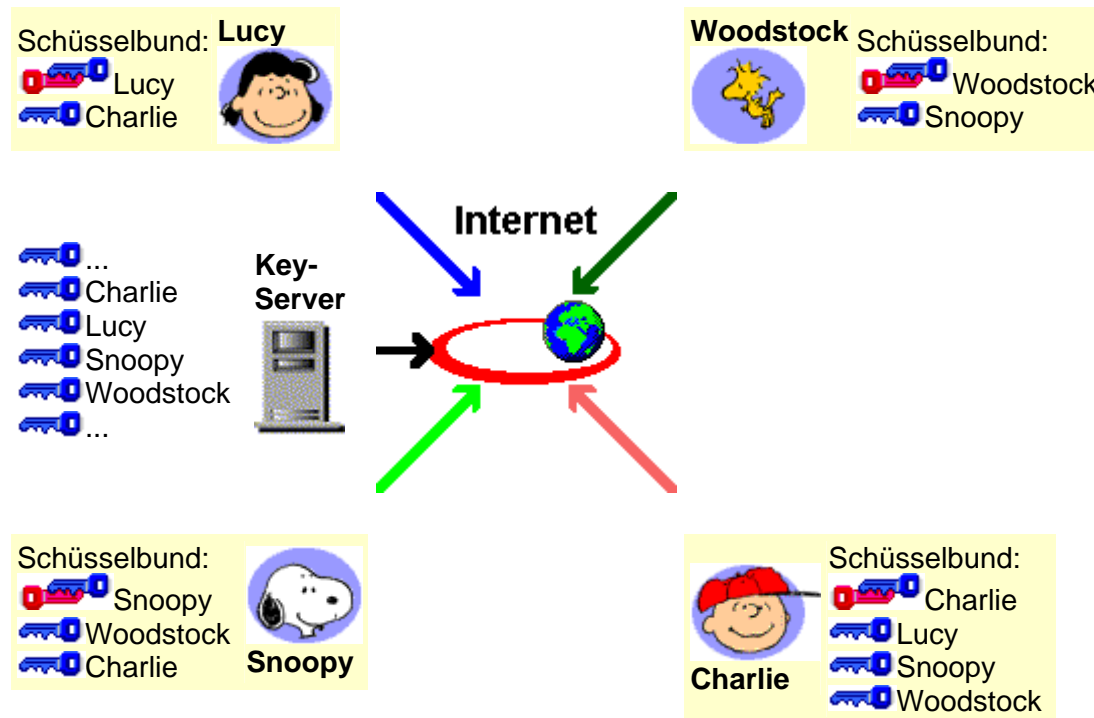
Wie das Schlüssel-Verschicken im Einzelnen geht, erfahren Sie später.

Ihren **privaten Schlüssel** dagegen behalten Sie auf Ihrem Rechner und achten darauf, dass er nicht in falsche Hände gerät.

Eine Verschlüsselung kann nur erfolgen, wenn der Empfängerschlüssel vorhanden ist.

Dieser wird dazu genutzt die E-Mail mit dem Empfängerschlüssel zu verschlüsseln und nur der Empfänger hat den richtigen Gegenschlüssel zum entschlüsseln der E-Mail.

Beispiel



Wenn Lucy eine **verschlüsselte E-Mail an Charly** schicken will, benötigt sie **seinen öffentlichen Schlüssel**. Den öffentlichen Schlüssel bekommt Lucy von Charly. Diesen Schlüssel verwaltet Lucy an ihrem Schlüsselbund.

Mit **seinem öffentlichen Schlüssel** kann Lucy eine E-Mail an Charly verschlüsseln. Nur Charly kann diese E-mail mit **seinem privaten Schlüssel** öffnen.

In dem Beispiel kann Charly an Lucy, Snoopy und Woodstock verschlüsselte E-Mail senden, Woodstock nur an Snoopy.

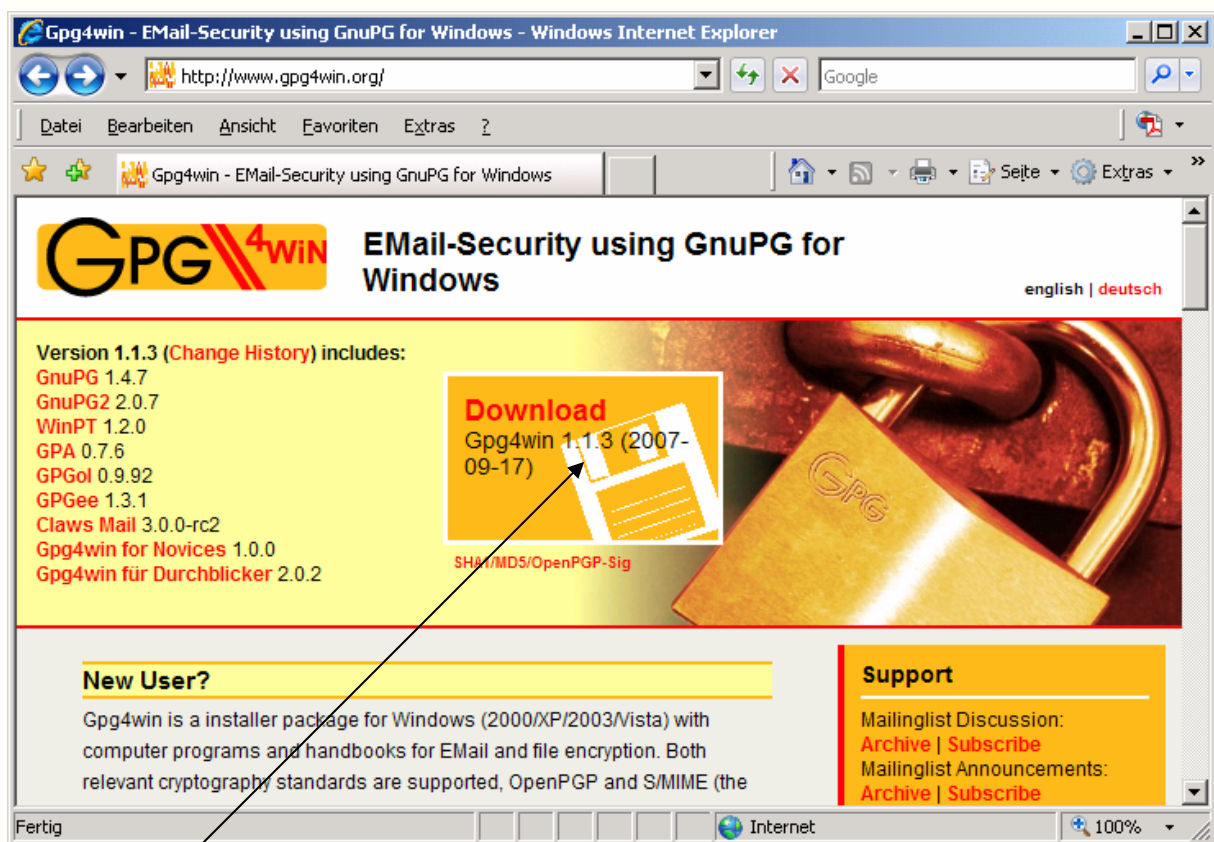
Die gesammelten öffentlichen Schlüssel werden zusammen mit der zugehörigen E-Mail-Adresse auf dem eigenen Rechner gespeichert und in der Schlüsselverwaltung aufgenommen. Es können Unmengen von öffentlichen Schlüssel aufgenommen und den jeweiligen e-mail Adressen zugeordnet.

Wie kann ich das System installieren und nutzen.

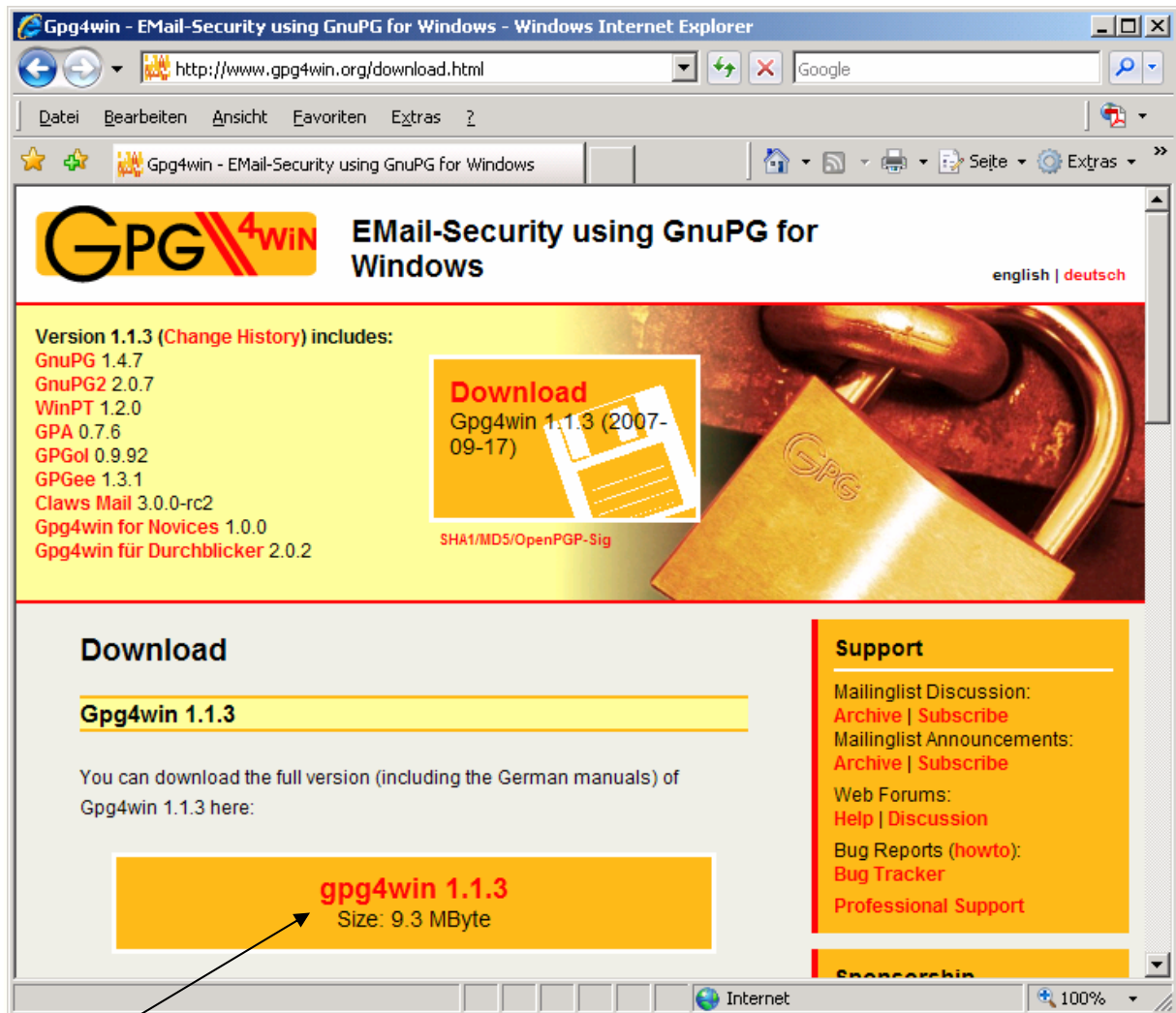
Erstes wird ein Verschlüsselungsprogramm benötigt:

Ich habe mich für das GnuPG Programm entschieden, da es sich um eine freie Software handelt: Für Jedermann ohne Kopierschutz zugänglich und kann gratis ohne Erlaubnis an jeden weiter gereicht werden.

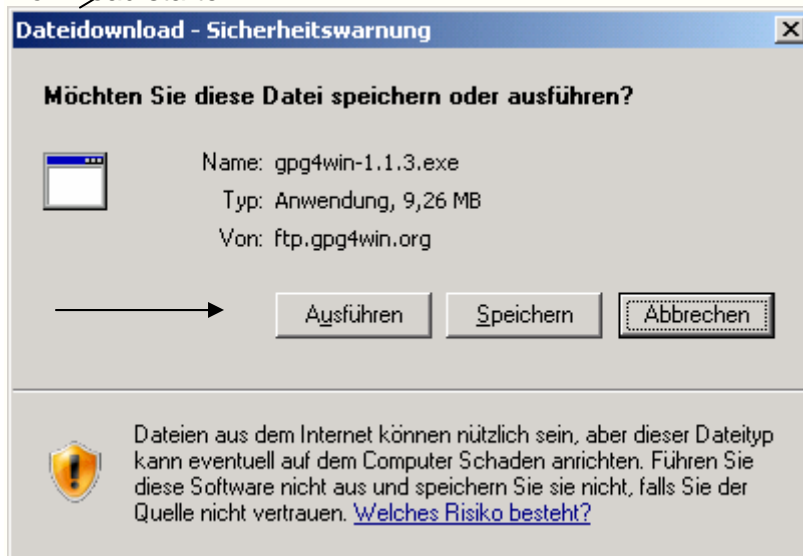
Seite aufrufen <http://www.gpg4win.org/>



Download von Gpgwin 1.1.3 aufrufen



Download starten



Gleich die Ausführung starten, wenn Sie das Programm nicht weiter geben möchten. Die Installation durchlaufen lassen.

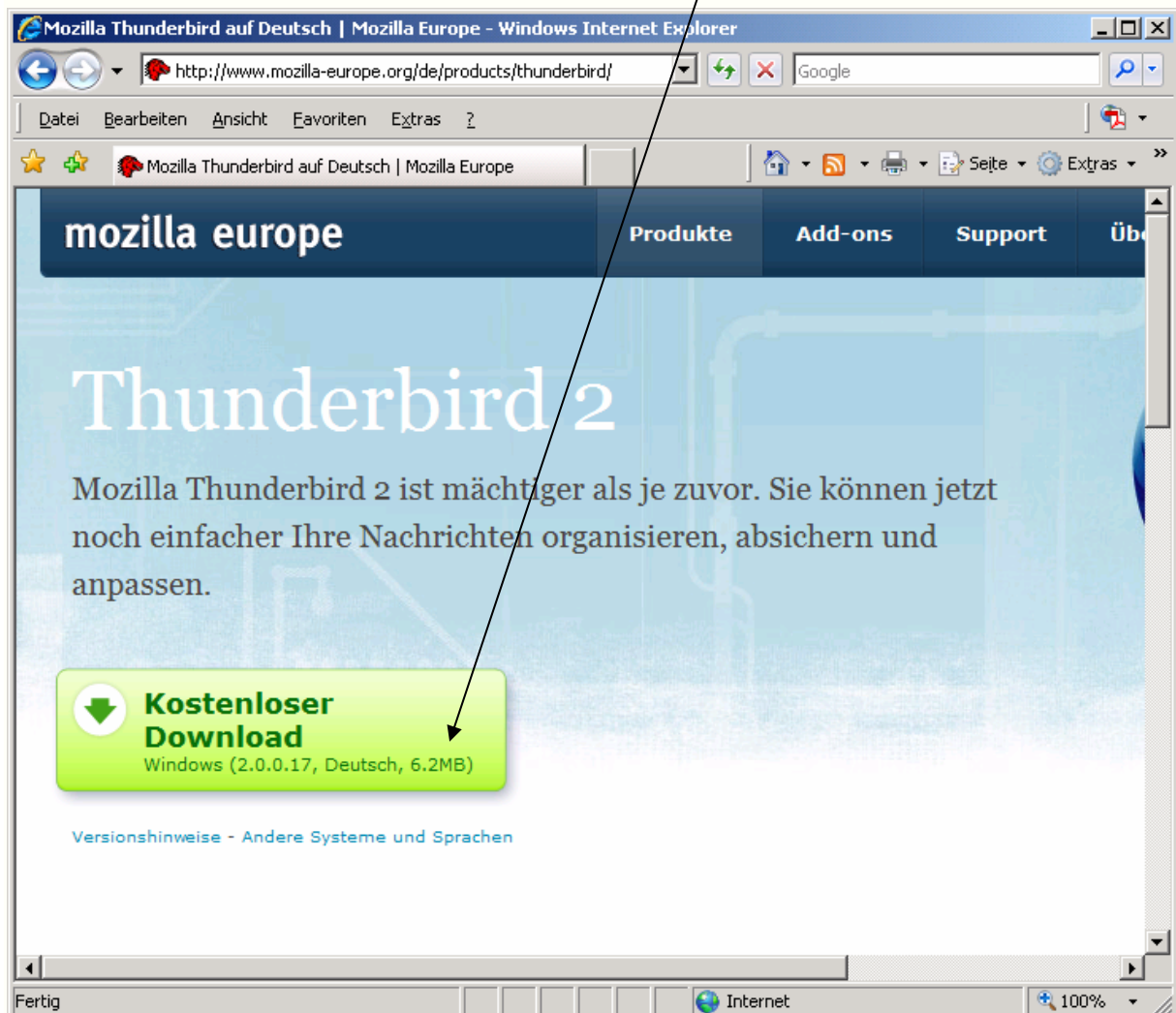
Zweitens benötigen Sie ein E-Mail Programm

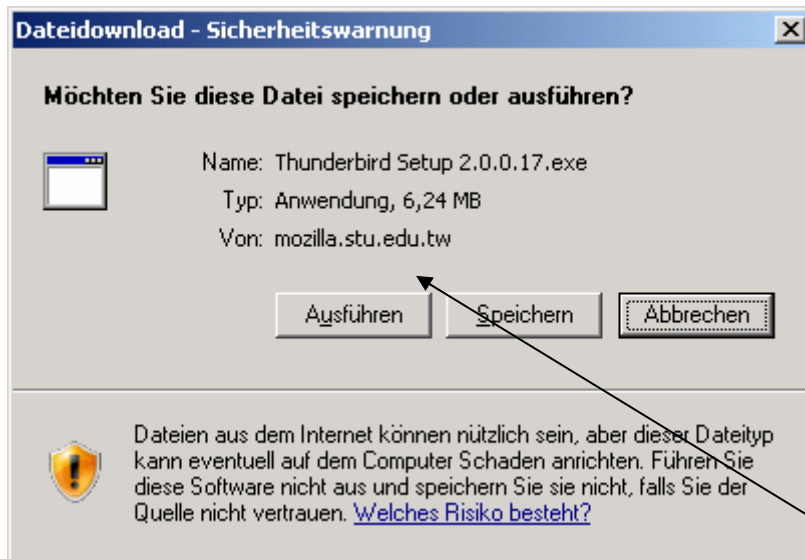
Ich habe mich für das Programm Thunderbird entschieden.

Das Programm kann kostenfrei vom Internet geladen werden

<http://www.mozilla-europe.org/de/products/thunderbird/>

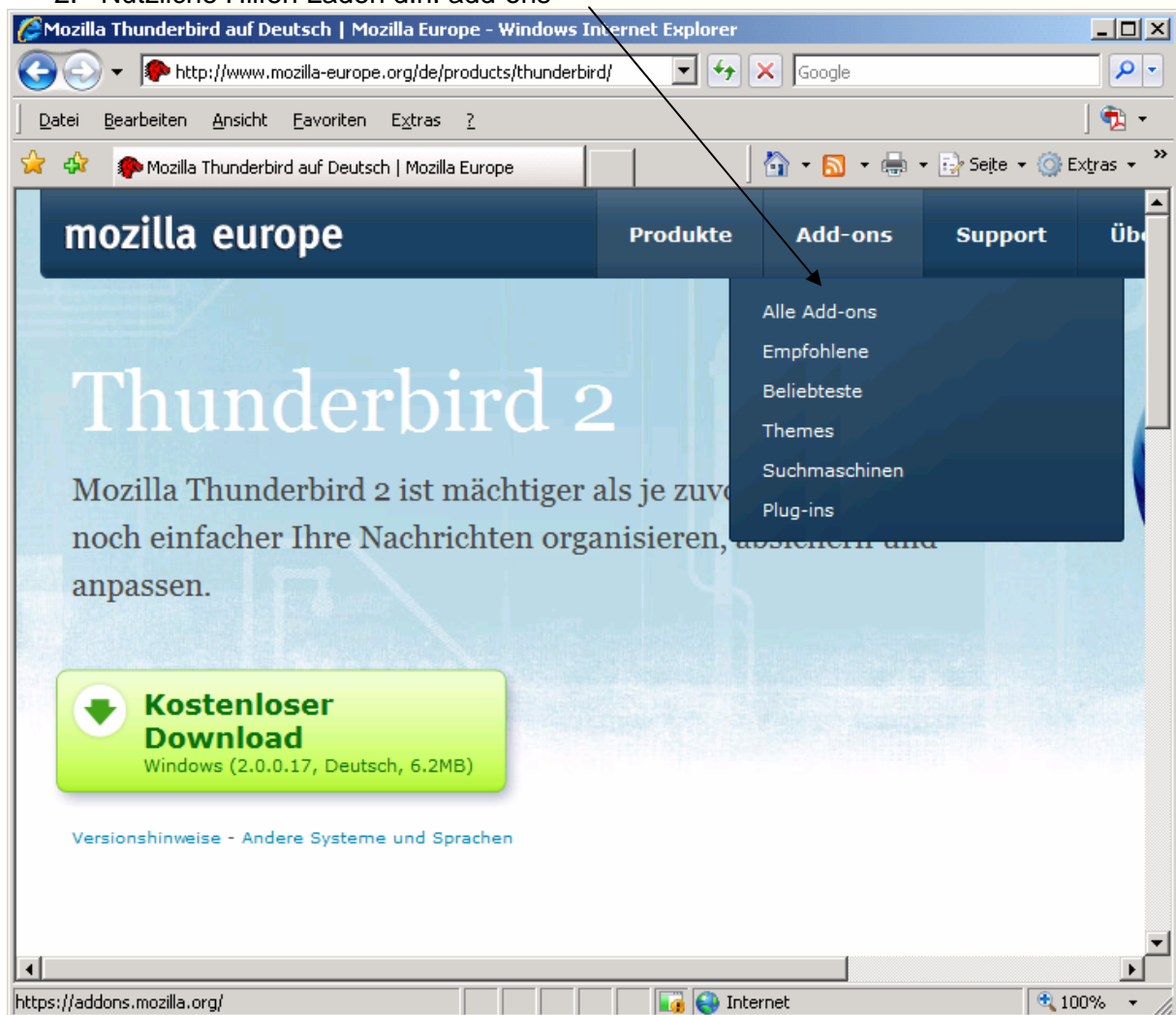
1. Das Programm herunterladen und ausführen





Gleich das Programm ausführen und die Installation durchführen und alle Daten aus Outlook importieren

2. Nützliche Hilfen Laden d.h. add-ons

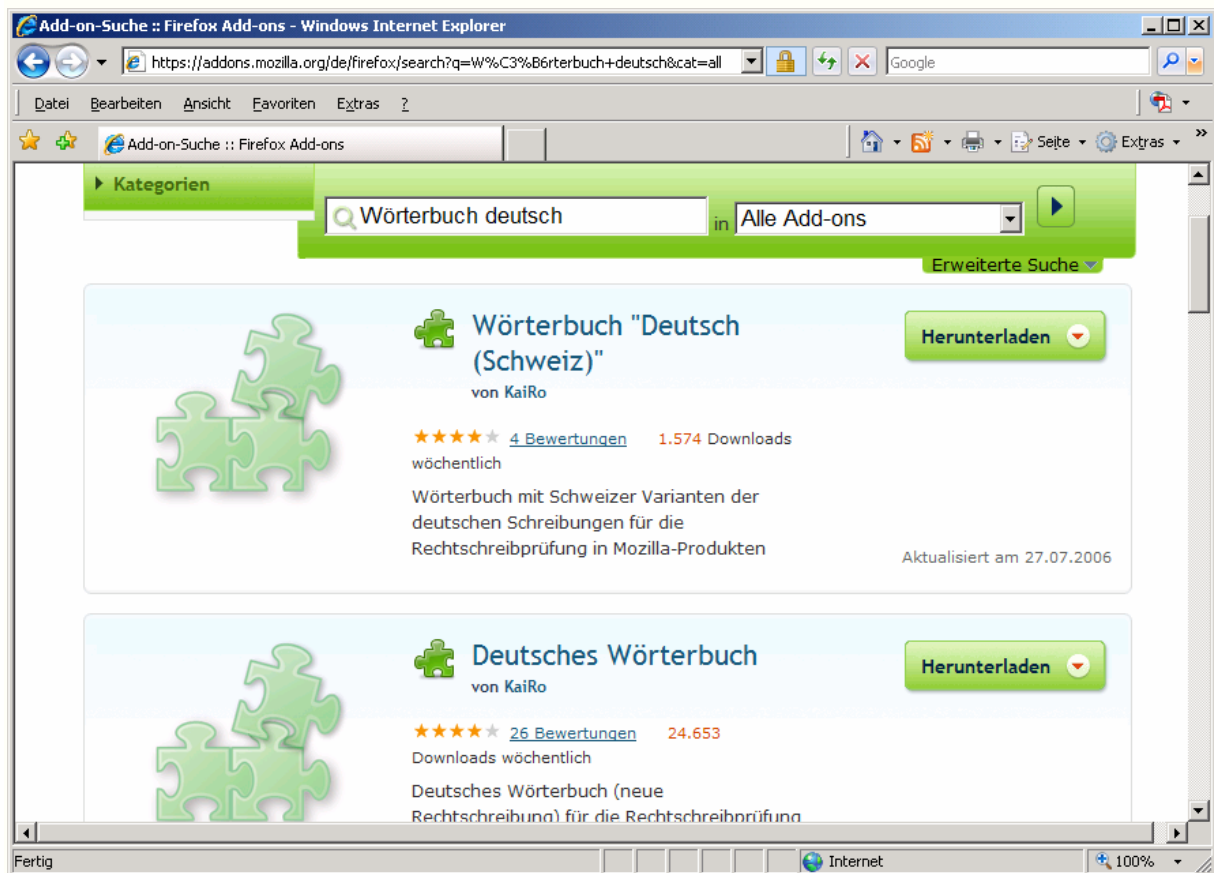


a. Enigmail wählen



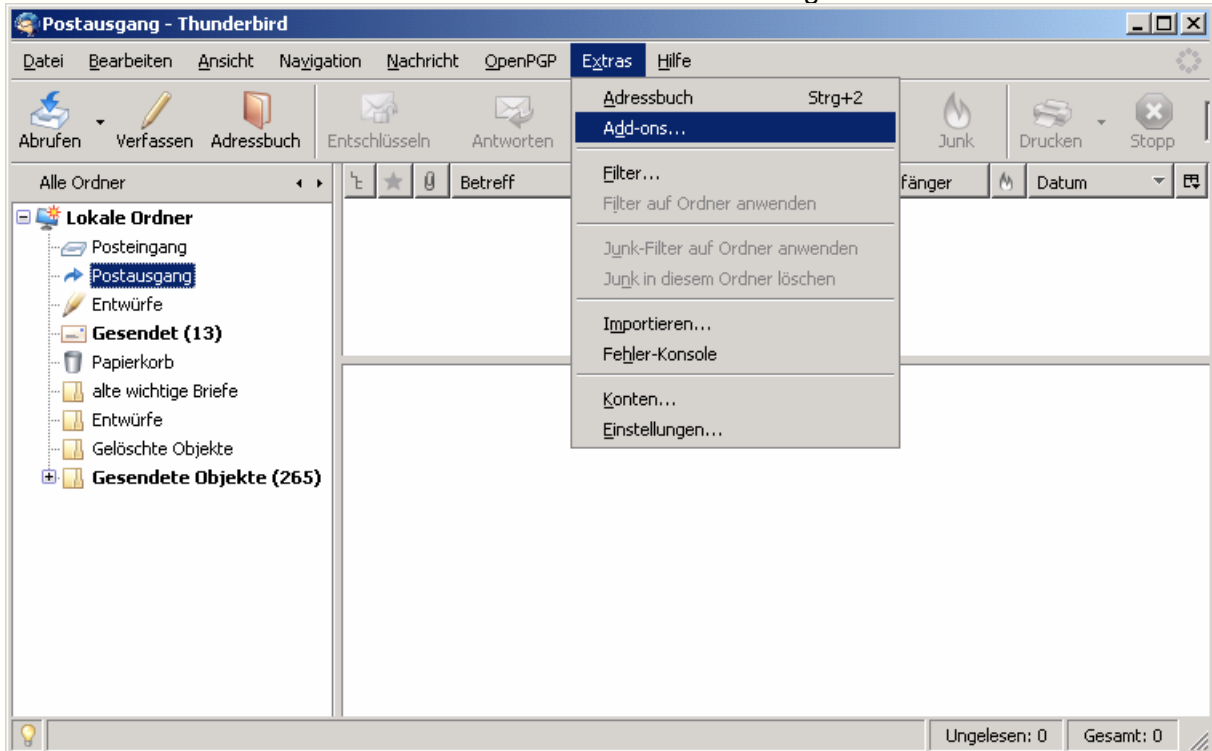
Download vornehmen und speichern, bitte beachten Sie bei der Speicherung wohin diese gespeichert werden, damit die Dateien später gefunden werden können.

b. Wörterbuch Deutsch

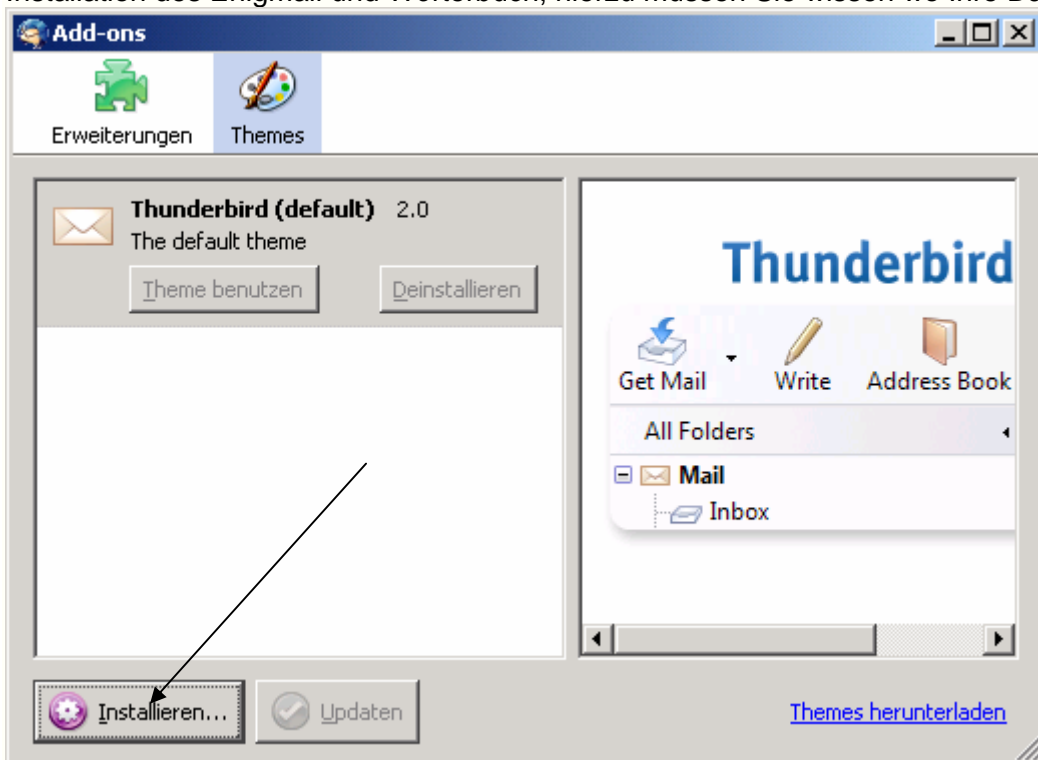


Download vornehmen und speichern, bitte beachten Sie bei der Speicherung wohin diese gespeichert werden, damit die Dateien später gefunden werden können.

4. Über den Bereich Extras add-ons können diese Erweiterungen installiert werden.



Installation des Enigmail und Wörterbuch, hierzu müssen Sie wissen wo Ihre Dateien sind.



Den Assistenten für Enigmail bitte nicht nutzen sonder über EXTRA Konto Einstellungen vornehmen.

Schlüsselerstellung

Öffnen Sie über START// PROGRAMME //GnuPG für Windows //WinPT.

Beim öffnen des Programms werden Sie gefragt ob ein Schlüssel erstellt werden soll, dies bejahen Sie.

Schlüsselerzeugungs-Assistent

Name und E-Mail Zuweisung

Jedes Schlüsselpaar muss einen eindeutigen Namen haben. Der Name und die E-Mail-Adresse dienen dazu das Korrespondenten wissen das der Schlüssel zu Ihnen gehört.

Ihr Name:

Mit der Zuweisung einer E-Mail-Adresse zu Ihrem Schlüsselpaar wird sichergestellt das WinPT den Korrespondenten assistieren kann den korrekten Schlüssel auswählen

E-Mail-Adresse

RSA Schlüssel bevorzugen

OK Abbrechen

Geben Sie Name und E-Mail-Adresse ein

Schlüsselerzeugung

Passwort eingeben

Maskiere Eingabe

OK Abbrechen

Bitte schreiben Sie sich Ihr Passwort auf!!! Dies wird benötigt um den verschlüsselten Postversand korrekt durchzuführen.

Jetzt wird für Sie das Schlüsselpaar erstellt.

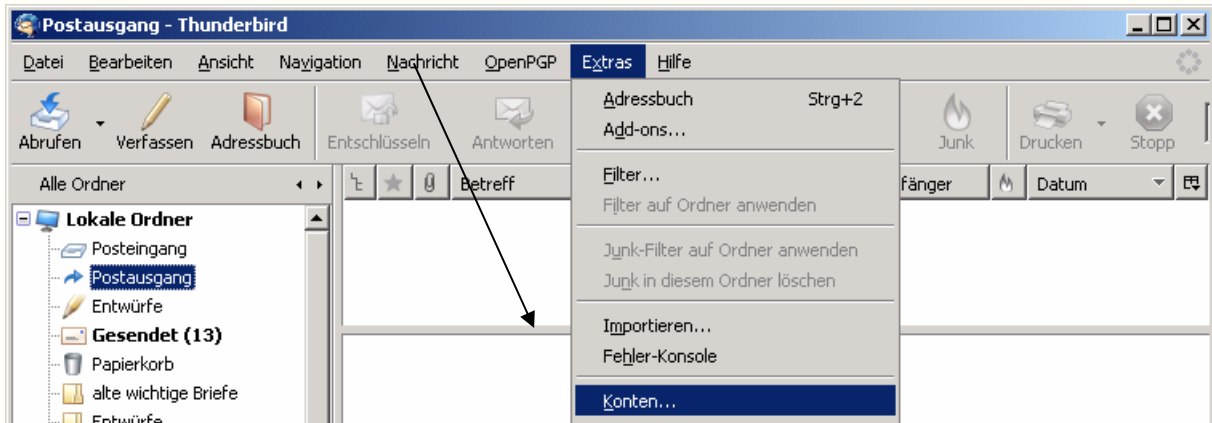
der öffentliche Schlüssel und
der private Schlüssel

Sie können das Programm verlassen und sich dem E-Mail Programm zuwenden.

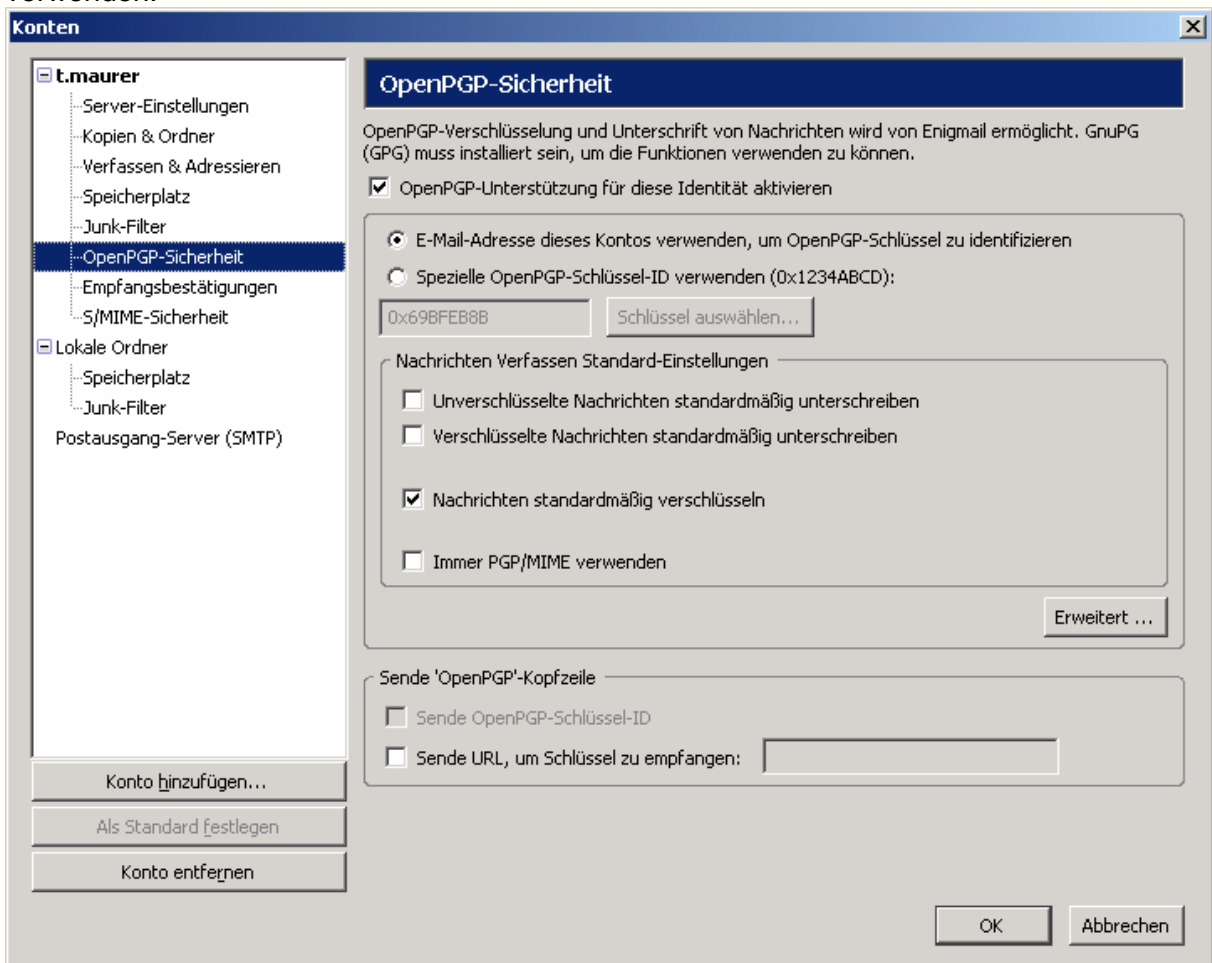
E-Mail Programm

Öffnen Sie das E-Mail Programm über START //PROGRAMM //Mozilla Thunderbird// Mozilla Thunderbird

Sie werden beim Öffnen gefragt ob Sie den Enigmail Assistent benötigen, bitte nicht benutzen. Öffnen Sie EXTRAS



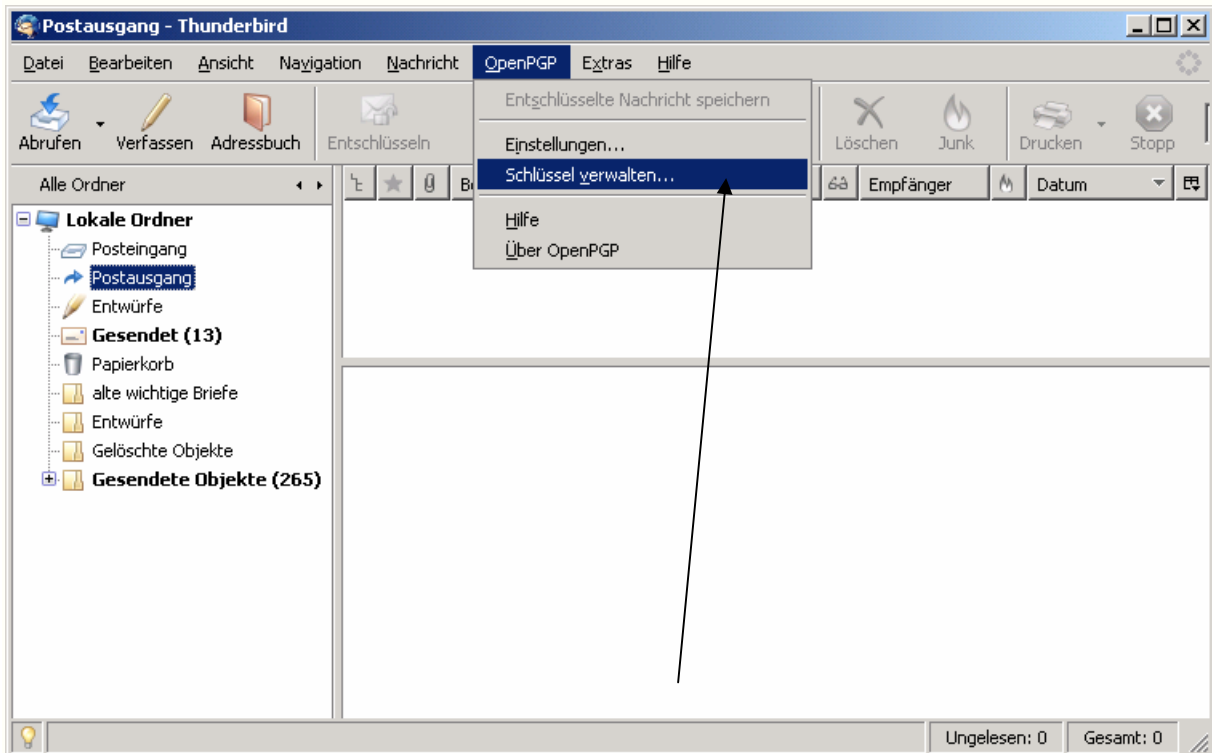
Und ändern die Einstellungen bei OpenPGP mit Haken bei E-Mail-Adresse diese Konto verwenden.



Schlüsselversendung

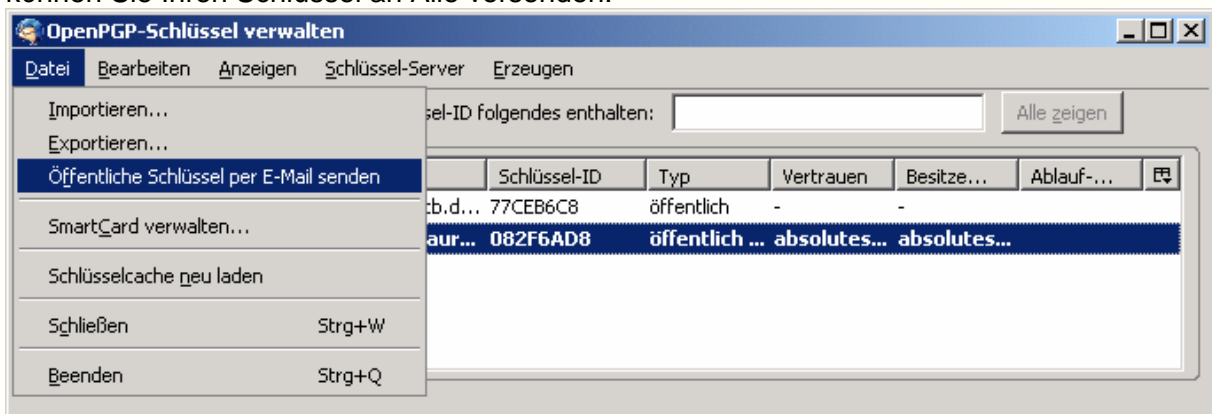
Jetzt müssen Sie nur noch Ihren öffentlichen Schlüssel versenden, damit Sie von anderen verschlüsselte E-Mail erhalten können.

Öffnen Sie über START //PROGRAMM //Mozilla Thunderbird// Mozilla Thunderbird



Öffnen Sie über OpenPGP, das Schlüssel verwalten.

Markieren Sie Ihren Schlüssel und über Datei Öffentliche Schlüssel per E-Mail senden können Sie Ihren Schlüssel an Alle versenden.

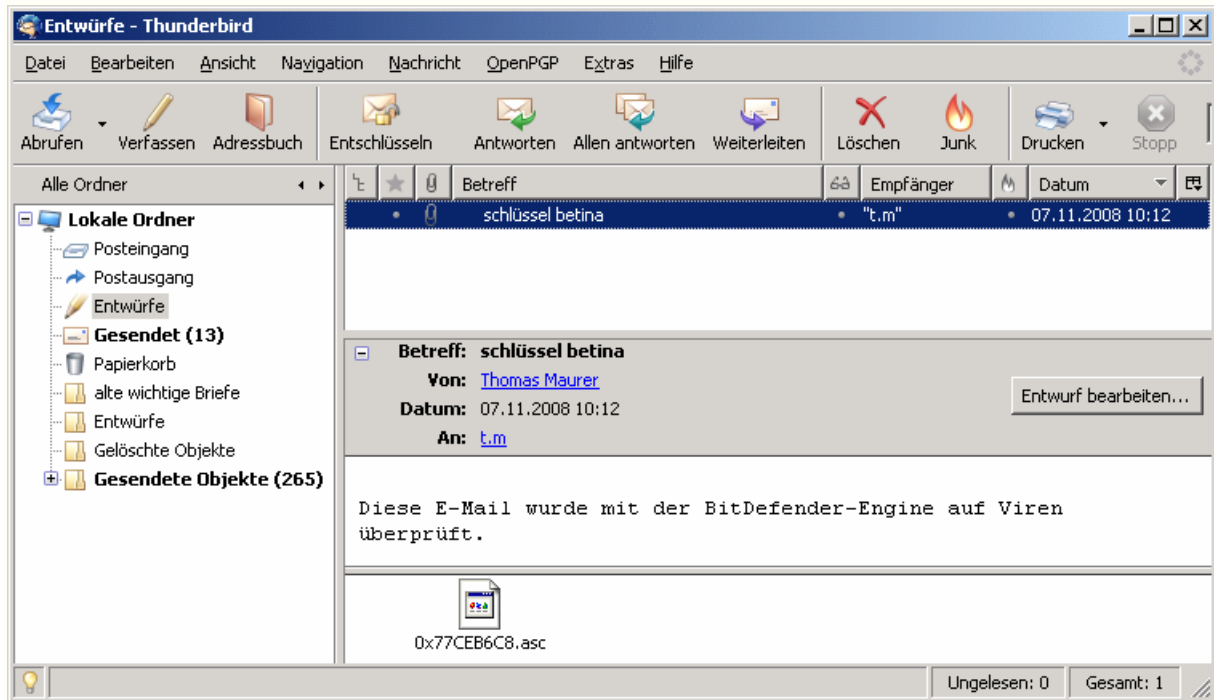


Nun kann Ihnen eine verschlüsselte E-mail zugesandt werden. Voraussetzung ist, dass der Versender den Schlüssel lesen und verwenden kann d.h. auch ein Verschlüsselungsprogramm besitzt.

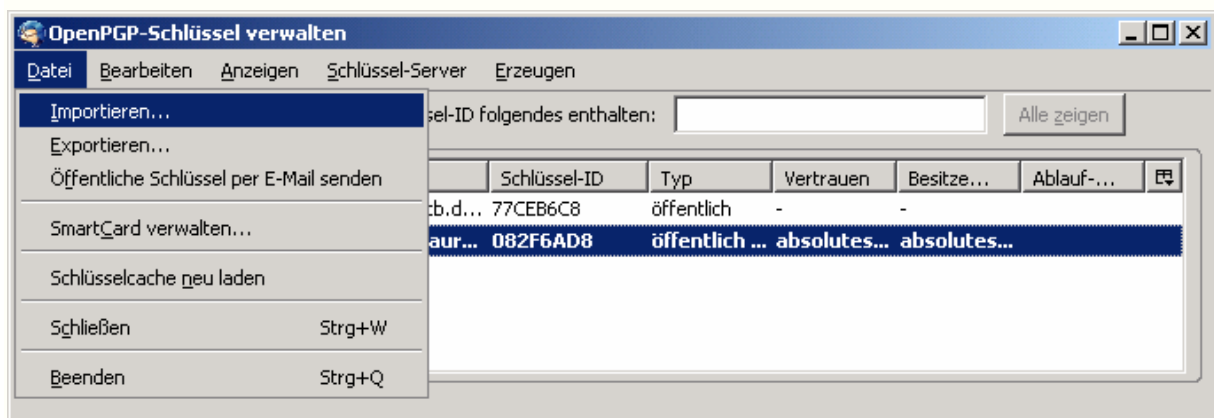
Empfangen von öffentlichen Schlüssel

Öffnen Sie über START //PROGRAMM //Mozilla Thunderbird// Mozilla Thunderbird

Rufen Sie die E-Mails ab



Speichern Sie den Anhang auf Ihrem Rechner (Bitte achten Sie darauf wohin). Öffnen Sie OpenPGP und die Schlüsselverwaltung.

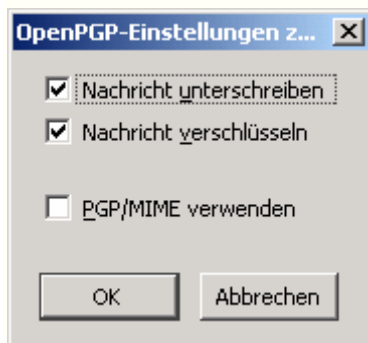


Über Datei Import können Sie den erhaltenen Schlüssel einspielen, dh. die vorhin gespeicherte Datei einspielen.

Versenden von E-Mail

Das versenden von E-Mail wird über den Button Verfassen ausgelöst. Die E-Mail wird wie gewohnt geschrieben bzw. Anhänge vorgenommen.

Beim versenden wird vorher der Punkt GnuPG aufgerufen und gewählt ob eine Unterschrift oder Verschlüsselung vorgenommen werden soll.



Im Fall, dass der Empfänger zur E-Mail-Adresse noch nicht zugeordnet wurde erscheint die Schlüsselauswahl. Jetzt muss der Empfängerschlüssel gewählt werden um die Verschlüsselung vorzunehmen.

