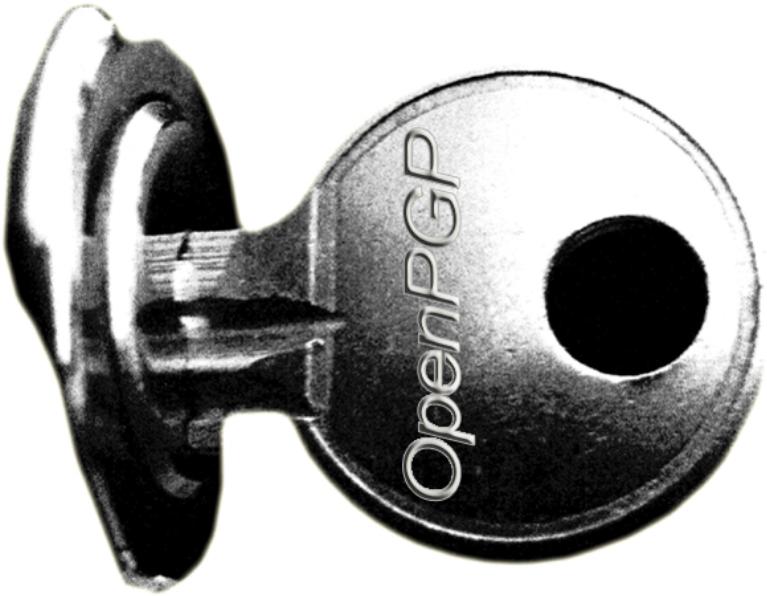
Sichere E-Mails mit GnuPG

Verschlüsselung und Signatur

von Salvatore Spadaro



Autor : Salvatore Spadaro

Version: 0.1.1 beta
Datum : 6. Dezember 2005

1 Weshalb sich Gedanken über Sicherheit machen? 3

2 Was ist Verschlüsselung? 5
2.1 symmetrische & asymmetrische Verschlüsselung 6
2.2 Vorteile & Nachteile der beiden Verfahren 6
2.3 Hybride Verschlüsselung 6

3 Was ist eine kryptografische Signatur? 7

4 Welche Krypto-Tools brauche ich? 9
4.1 Was ist GnuPG? 9
4.2 Warum geht diese Anleitung nicht auf PGP ein? 9

5 Installation von GnuPT-Light 10

6 Thunderbird Enigmail 14
6.1 Erstellung eines Keyrings 14
6.2 Erstellung eines Widerrufs-Zertifikats 18
6.3 Public Key auf Keyserver kopieren 19
6.4 Mails signieren 23
6.5 Mails verschlüsseln 26

7 Quellenangeben 28
7.1 Print-Medien 28
7.2 Internet 28
7.3 Grafiken 28

1 Weshalb sich Gedanken über Sicherheit machen?

"The security of electronic mail sent through the Internet may be described in exact three words: there is none." - Matt Bishop

Viele Leute fragen sich wozu sie den Mehr-Aufwand für die Einrichtung von Verschlüsselungs-Systemen wie GnuPG oder PGP betreiben sollen. PC-Lainen tun sich gewöhnlicherweise sehr schwer sich in das Thema Kryptografie bzw. Mail-Security einzuarbeiten – sie werden meist ohne Erklärungen oder gar Hilfestellungen mit Begriffen wie „RSA“, „IDEA“, „Public Key“ u.a konfrontiert. Oft hört sich dieses Fachchinesisch viel komplizierter an als es ist. Sie müssen weder Kryptologe noch Informatiker sein um Ihre Mails zu verschlüsseln oder zu signieren – mit Hilfe dieser Anleitung wird es Ihnen möglich sein für ein gewisses Maß an Sicherheit zu sorgen.

Jetzt aber zurück zur zentralen Frage „Warum sollte man sich Gedanken über Sicherheit und Verschlüsselung machen?“. Nun, die Frage wurde eigentlich bereits durch das Zitat von Matt Bishop beantwortet, die Sicherheit des Internets und damit auch des Mail-Verkehrs kann tatsächlich mit 3 Worten beschrieben werden: „Es gibt keine“. Unter Berücksichtigung kryptografischer Signier- und Verschlüsselungsmethoden ist zwar immer noch keine 100-prozentige Sicherheit gegeben, es ist aber Unterschied, ob Sie Bargeld in einem Schaufenster sichtbar aufbewahren oder es zu Hause in einem Möbeltresor verstecken. Der Versand von E-Mails verhält sich ähnlich wie das genannte Beispiel mit dem Geld – wird eine E-Mail verschickt, passiert sie einige Zwischenstationen ähnlich wie ein gewönlicher Brief, nur das es sich bei der E-Mail um Knotenpunkte und Router handelt und nicht um Brief- und Frachtzentren der deutschen Post.

Der Haken an der Sache ist, dass E-Mails standardmäßig im Reintext übertragen werden und sich ohne größeren Aufwand von neugierigen Personen oder Hackern, abfangen, lesen oder sogar manipulieren lassen. Oft werden über solche Vorgehensweisen Viren in Netzwerke eingeschleust oder in schlimmeren Fällen Industriespionage betrieben, in diesen Fällen spricht man von der sogenannten „Men-in-the-Middle-Attack“, wobei sich ein Spion mit Hilfe von spezieller Software bewusst zwischen den Sender und dem Empfänger einklinken kann um alle Informationen abzuhören.

Auch wenn die Mail-Korrespondenz privat ist, wollen Sie bestimmt nicht, dass sich Fremde Ihre Liebesbriefe unter den Nagel reisen oder sich als Ihre Freunde oder Bekannte ausgeben um an wichtige Informationen heranzukommen (Stichwort Social Engineering). Oder etwa doch? Oftmals werden vertraute Nachrichten wie z.B. wichtige Bestellungen, Rechnungen, Formulare usw. per Mail verschickt - meistens ist dem User leider nicht bewusst welche Auswirkungen eine unsichere Mail-Kommunikation haben kann.
Will man die private oder geschäftliche E-Mailkorrospondenz sicherer gestalten sollte man sich mit den beiden kryptografischen Verfahren, Verschlüsselung und Signierung beschäftigen und mit Hilfe sogenannter „Krypto-Tools“ welche noch beschrieben werden auseinander setzen.

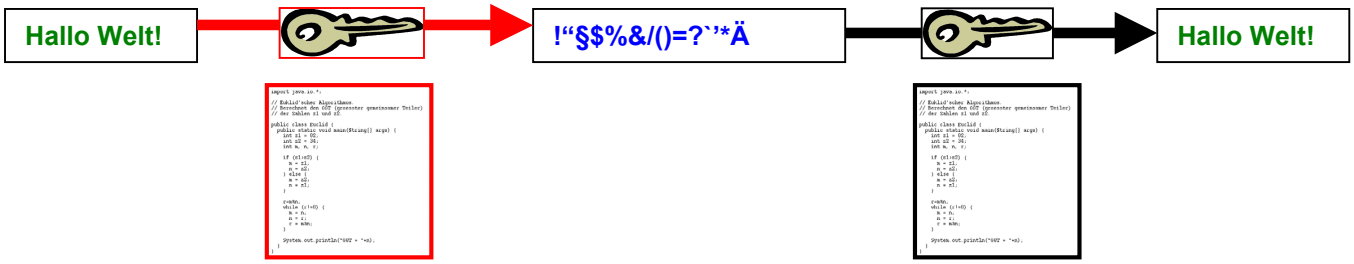
.

2 Was ist Verschlüsselung?

Die Verschlüsselung wird eingesetzt um einen Klartext mit Hilfe eines bestimmten Verschlüsselungs-Algorithmus in einen codierten Text umzuwandeln, dabei kommen je nach Verschlüsselungsverfahren ein oder mehrere Schlüssel (Keys) zum Einsatz um die Botschaft wieder zu entschlüsseln.

Die Wissenschaft der Verschlüsselungsmethoden wird als Kryptografie bezeichnet. Das Forschungsgebiet Kyrptoanalyse beschäftigt sich hingegen ausschließlich mit der Entschlüsselung und Überprüfung kryptografischer Verfahren (Kryto-Algorithmen).

Bekannte Verschlüsselungsalgorithmen sind z.B. ElGamal, CAST5, Triple DES (3DES), AES (Rijndael), Blowfish, RSA, IDEA u.v.m.
In folgender Grafik wird Ihnen in vereinfachter Form, das Verschlüsselungschema dargestellt.



2.1 symmetrische & asymmetrische Verschlüsselung

Hauptunterschied zwischen „symmetrischer“ und „asymmetrischer“ Verschlüsselung ist, dass bei der symmetrischen Verschlüsselung nur 1 Schlüssel für die Ver- und Entschlüsselung zum Einsatz kommt. Die „asymmetrische“ Verschlüsselung hingegeben verwendet Public Key und Private Key.

2.2 Vorteile & Nachteile der beiden Verfahren

Hauptunterschied zwischen „symmetrischer“ und „asymmetrischer“ Verschlüsselung ist, dass bei der symmetrischen Verschlüsselung nur 1 Schlüssel für die Ver- und Entschlüsselung zum Einsatz kommt. Die „asymmetrische“ Verschlüsselung hingegeben verwendet Public Key und Private Key.

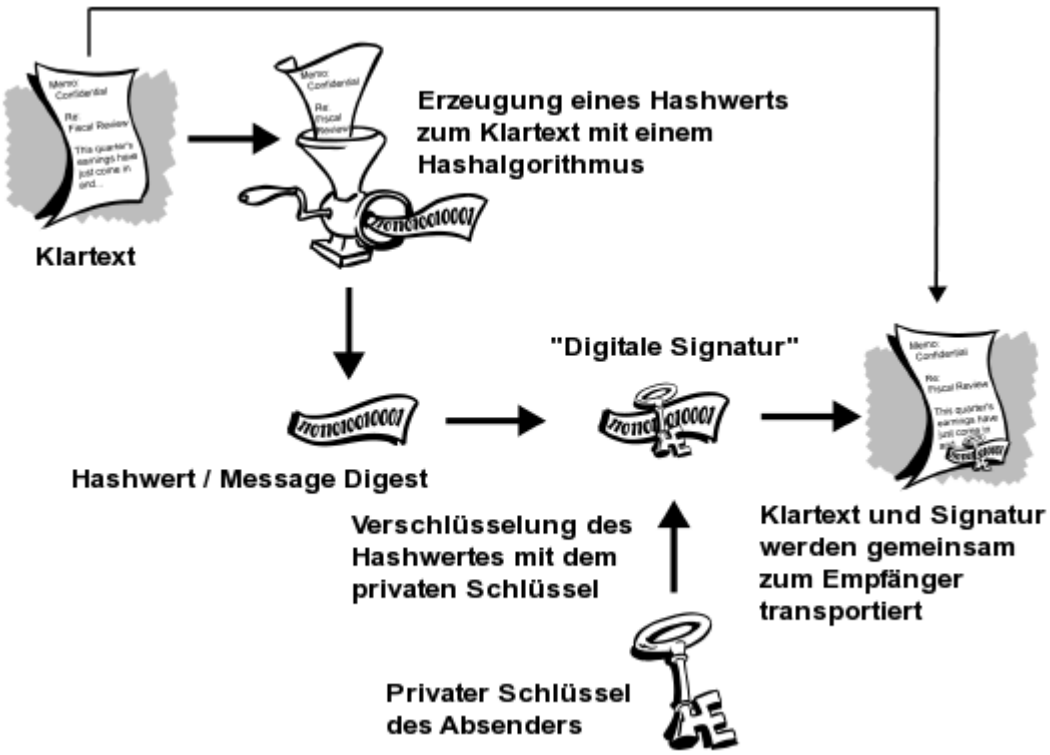
2.3 Hybride Verschlüsselung

Um die Vorteile der „symmetrischen“ & „asymmetrischen“ Verschlüsselung zu verbinden wurde das „Hypride Verschlüsselungsverfahren“ entwickelt, dieses kommt bei „GPG“ und „PGP“ zum Einsatz.

3 Was ist eine kryptografische Signatur?

Eine kryptografische Signatur dient in erster Linie dazu die Identität des Absenders sicherzustellen, so dass gefälschte E-Mails sofort erkannt werden können. Mit Hilfe des privaten Schlüssels wird ein sogenannter Hash-Wert (Prüfsumme) gebildet und mit der signierten E-Mail verschickt, der Empfänger besorgt sich anschließend den Public Key des Senders und bildet ebenfalls den Hash-Wert der Mail – stimmen die beiden Prüfsummen überein wird die E-Mail als vertrauenswürdig eingestuft, es kann davon ausgegangen werden das die E-Mail nicht gefälscht wurde.

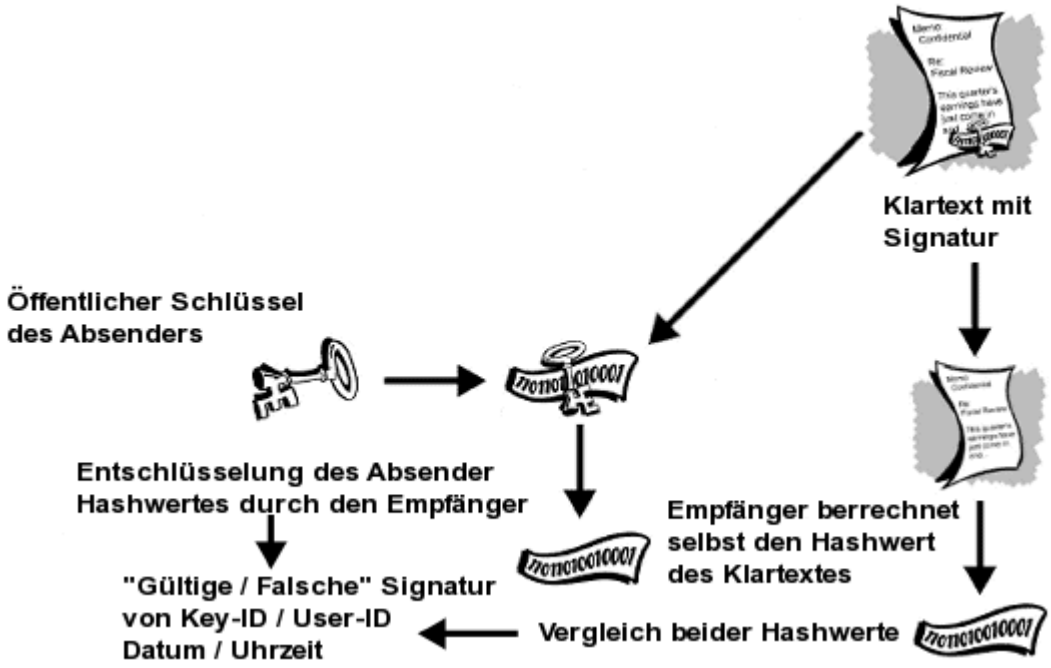
Signierung durch Absender:



Signierung durch Absender

Hinweis:
Die grafischen Abbildungen stammen aus der Anleitung Einführung in die Kryptographie von Network Associates, jetzt PGP Corporation, zu PGP 6.5.1 International.

Signaturprüfung durch Empfänger:



Signaturprüfung durch Empfänger

4 Welche Krypto-Tools brauche ich?

Für die E-Mail-Verschlüsselung/Signierung benötigt man drei Tools:

- GnuPG: übernimmt die Schlüssel-Erstellung
- Mozilla Thunderbird
- Enigmail: Plug-in für Thunderbird als GPG-Implementierung

Bevor Sie mit Thunderbird Enigmail einen Keyring erzeugen können, müssen Sie die Software GnuPG installieren, welche die Schlüsselerzeugung übernimmt. Mit Enigmail alleine können Sie noch keinen Schlüssel generieren! Die Schlüsselverwaltung des Tools WinPT (enthalten in der Krypto-Suite GnuPT) ist meiner Meinung nach besser als die Enigmail-Schluesselverwaltung wir empfehlen hnen trotzdem den Einsatz von GnuPT-Light, in diesem Paket ist die Schlüsselverwaltung WinPT nicht enthalten, der Grund warum wir Ihnen von WinPT abraten möchten, ist die Instabilität des Programms. Die aktuelle Version befindet sich noch im Entwicklungsstadium, bei Versuchen auf diversen Test-Rechnern kam zu Programm-Abstürzen.

4.1 Was ist GnuPG?

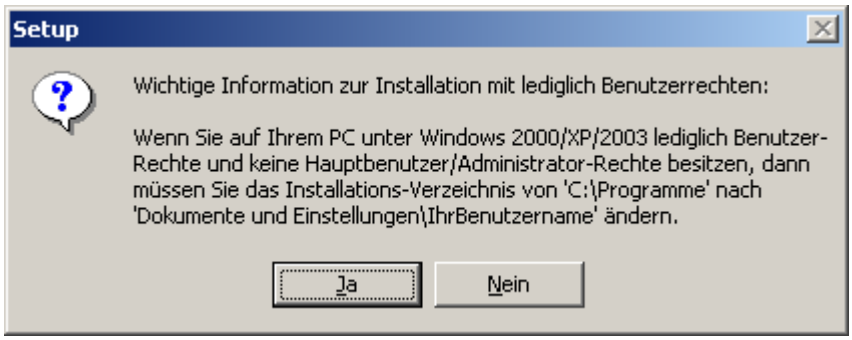
GnuPG läuft unter den meisten Betriebssystem, Linux, Windows, Mac OS etc. werden vollständig unterstützt. Das Programm wurde vom Bundesministerium für Wirtschaft und Arbeit (BMWA) und Bundesministerium für Inneres (BMI) unter der Aktion „Sicherheit im Internet“ finanziell gefördert um Verschlüsselung für jedermann zu ermöglichen.

4.2 Warum geht diese Anleitung nicht auf PGP ein?

PGP unterscheidet sich vom Funktionsprinzip von GPG kaum. Ein kravierender Nachteil zu GPG ist aber, dass PGP mit kommerziellen und teilweise nicht offen gelegten Verschlüsselungsverfahren arbeitet, dies ist eine gewisse Sicherheitslücke da die propritäre Software keinen Zugriff auf den Quellcode gewährt, dies bürgt immer die Gefahr von sog. Backdoors (Hintertüren).

5 Installation von GnuPT-Light

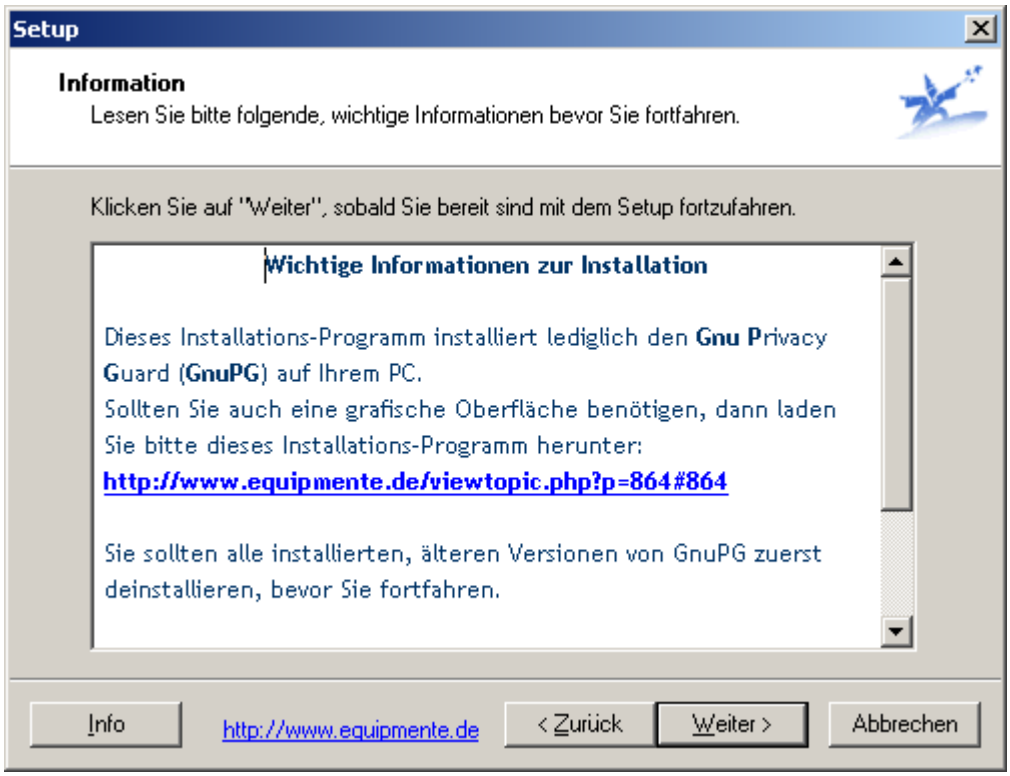
Gleich zu Beginn der GnuPT-Light-Installation werden Sie auf folgendes hingewiesen: Sollten Sie nicht als Hauptbenutzer/Administrator angemeldet sein, so muss der Installationsordner angepasst werden.



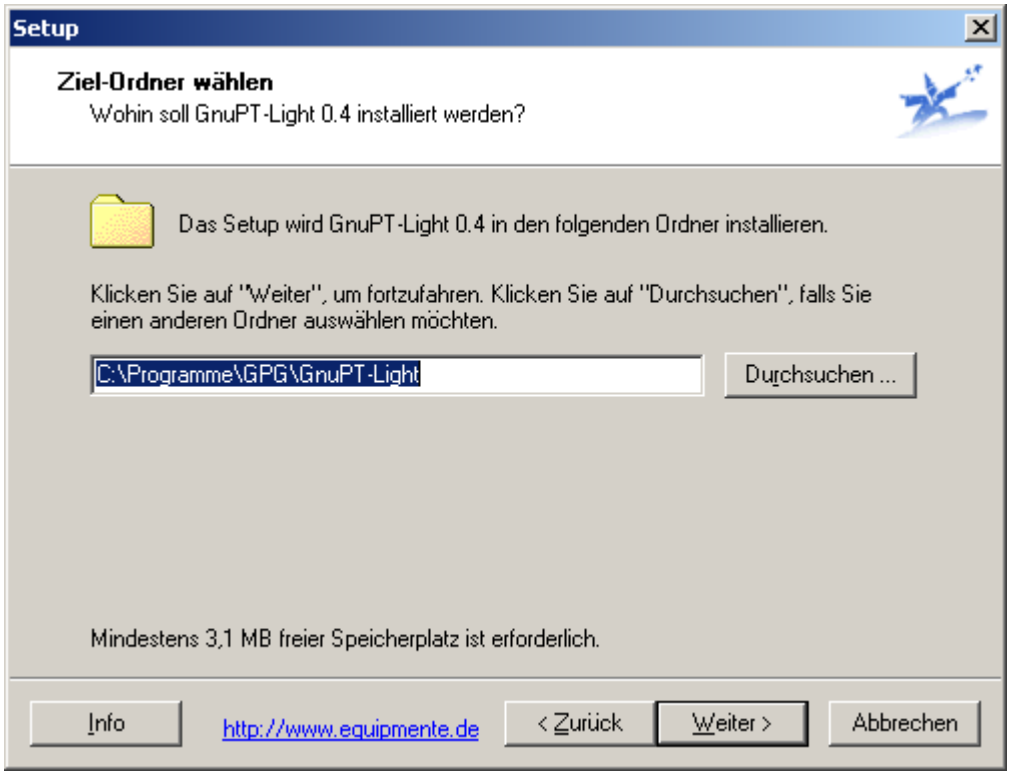
Klicken Sie auf „Weiter“ um mit der Installation fortzufahren:

Bitte die Lizenzbedingungen (GNU GPL) durchlesen und die Vereinbarung bestätigen:

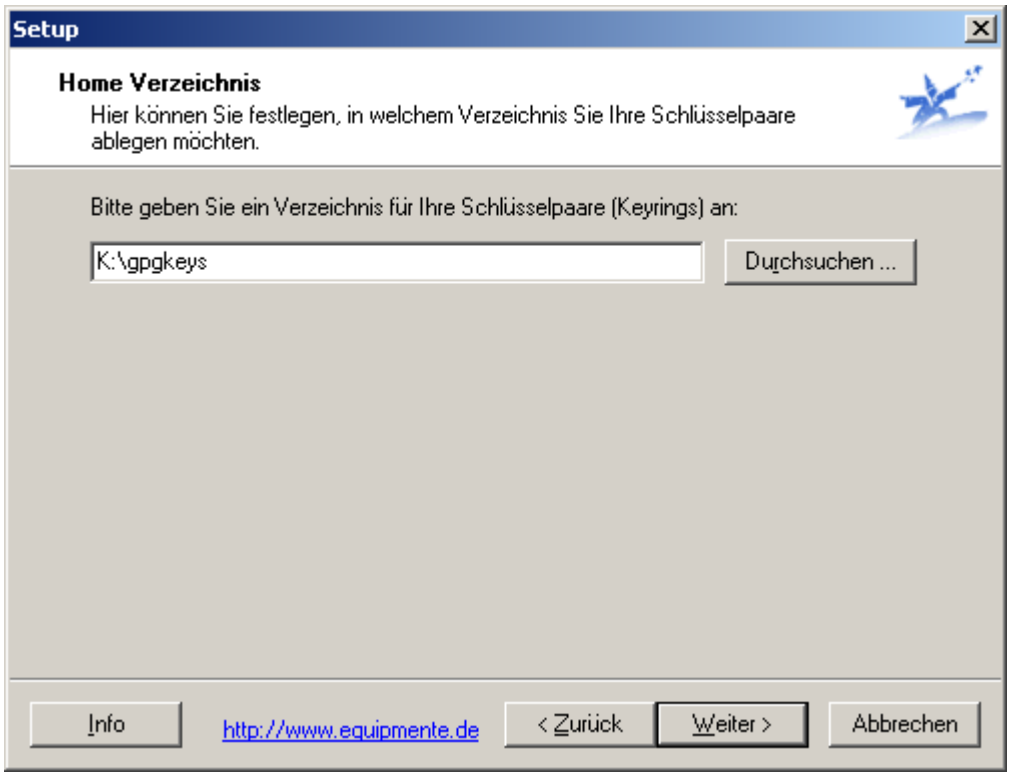
Nachfolgend erscheinen „Wichtige Informationen zur Installation“ die Sie sich bitte auch aufmerksam durchlesen. Weiter geht’s mit „Weiter“ ;-)



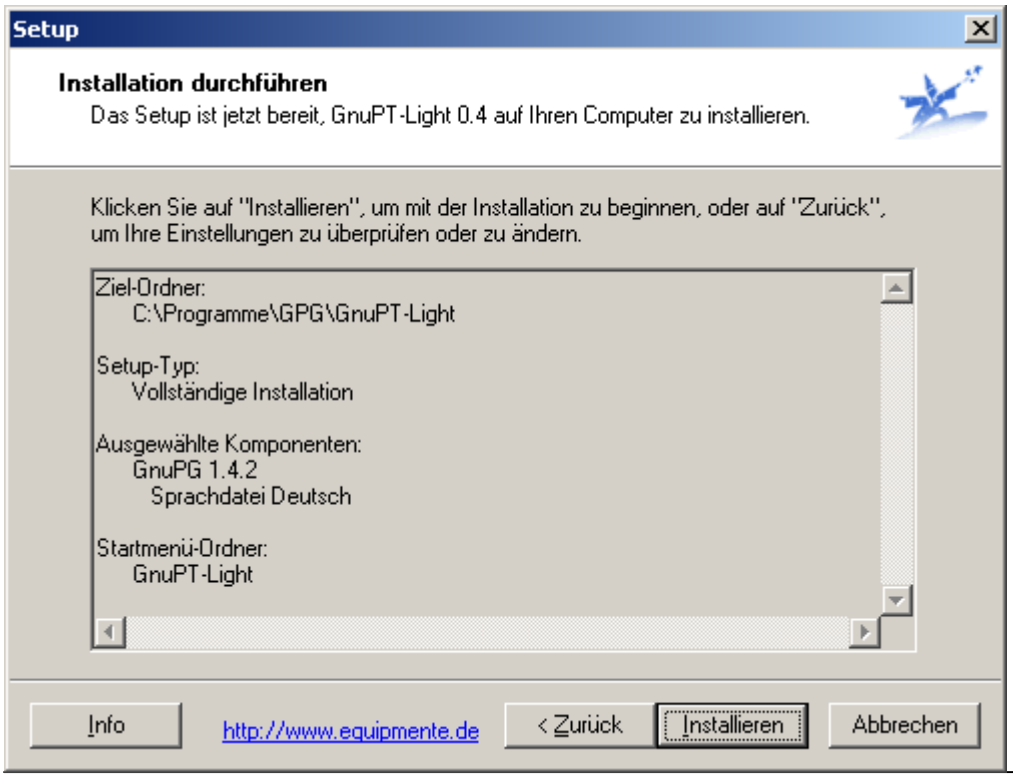
Bitte den Pfad für die Installation angeben (dieser kann je nach Konfiguration unterschiedlich sein)



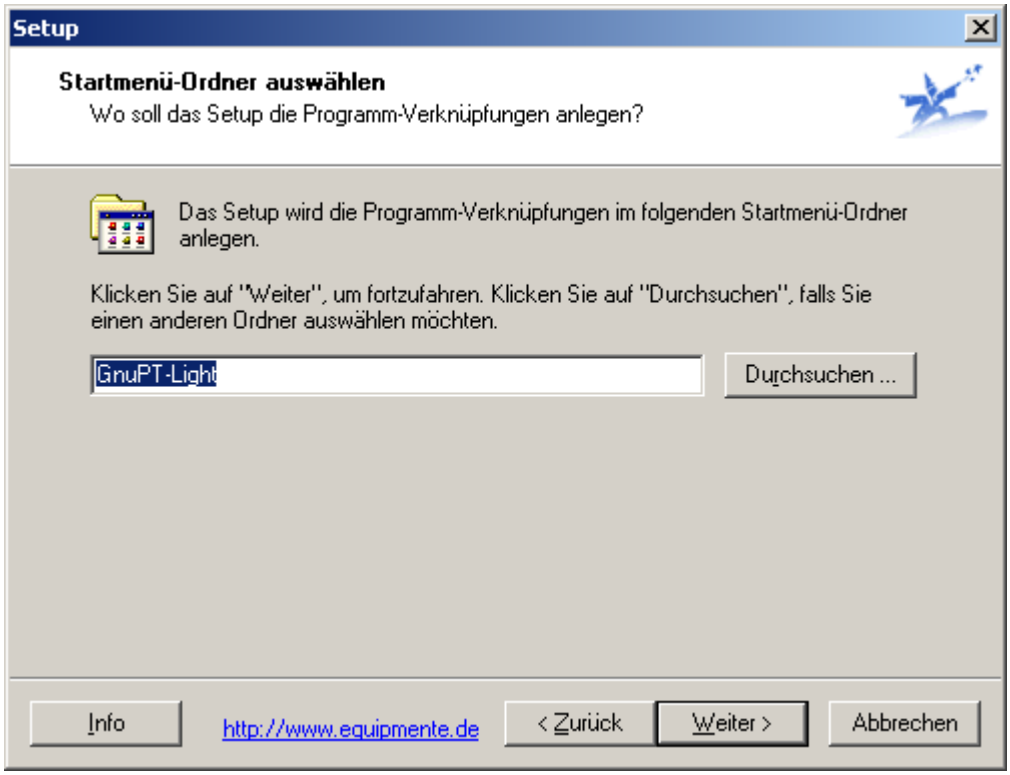
Falls Sie bereits über GPG-Schlüssel verfügen bitte das entsprechende Verzeichnis angeben, andernfalls ist es ratsam eines an einem sichern Ort (USB-Stick, Diskette etc.) zu erstellen.



Übersicht der Installations-Einstellungen:



Auswahl des Zielverzeichnisses für die GnuPT-Light-Verknüpfung (Startmenü).



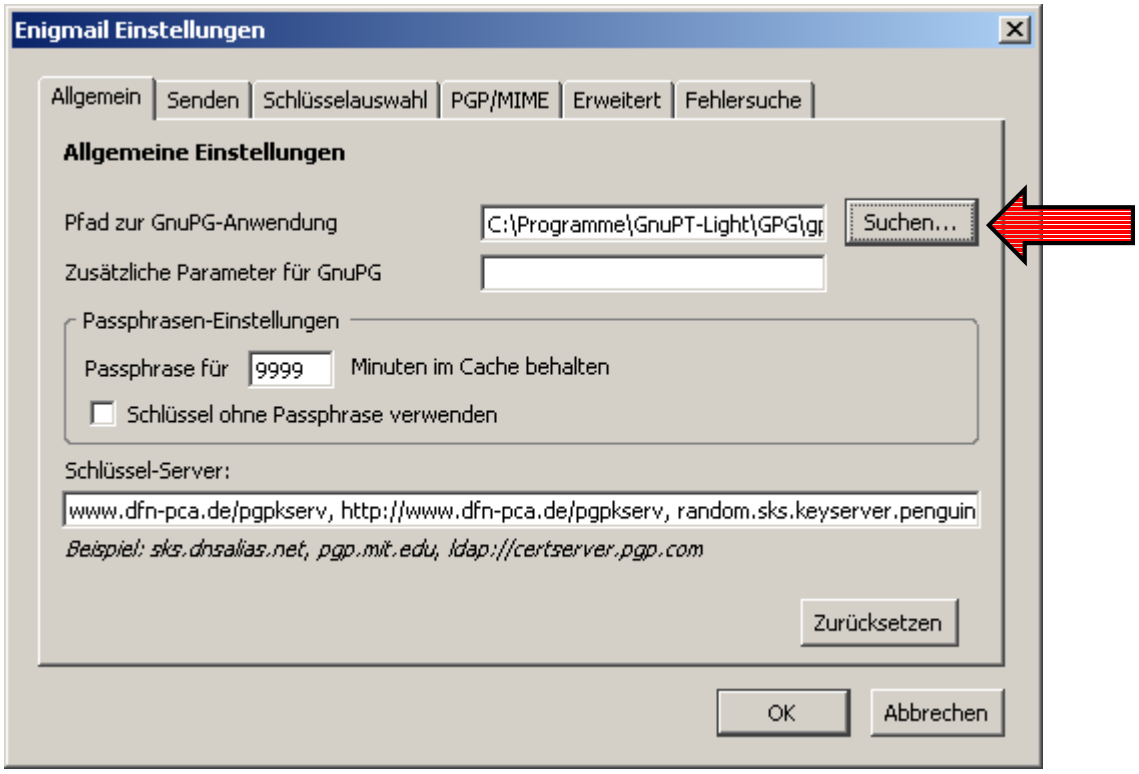
Am Ende der Installation erscheint noch ein Hinweisfenster das über die erfolgreiche Installation berichtet. Daneben können Sie sich noch Produktinfos ansehen (empfehlenswert falls Sie mit GnuPT nicht vertraut sind).

6 Thunderbird Enigmail

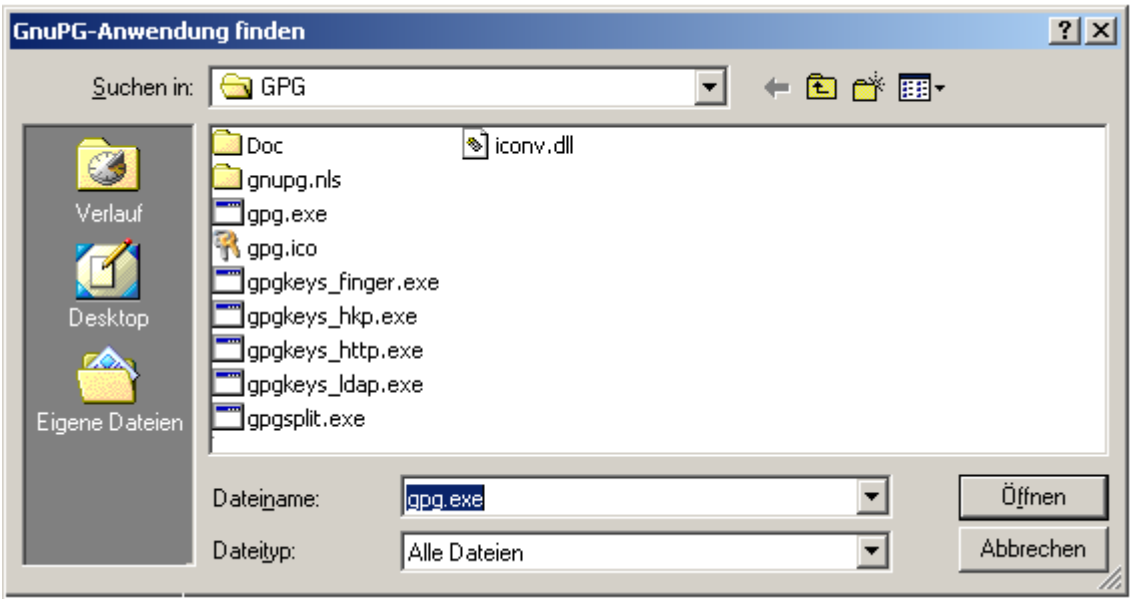
Wenn Sie E-Mails verschlüsseln und entschlüsseln möchten benötigen Sie einen Public Key und einen Private Key, diese beiden Schlüssel sind mathematisch gesehen voneinander abhängig, so dass es nicht ausreichend ist nur den geheimen privaten Schlüssel zu besitzen!
Damit keine Schlüssel verloren gehen werden diese in sog. Keyrings (Schlüsselbund) abgelegt – Private Keys werden dem Private Keyring hinzugefügt, Public Keys gehören dem Public Keyring an – neben den Schlüsseln werden auch Zertifikate und andere zugehörige Schlüsseldaten in den Keyrings abgespeichert – so ist es möglich den Public-Key mit einem persönlichen Foto zu versehen. In diesem Abschnitt ist beschrieben wie mit der Thunderbird-Erweiterung „Enigmail“ (integrierte Schlüsselverwaltung) eigene Keyrings für den gesicherten Mail-Verkehr angelegt werden können.

6.1 Erstellung eines Keyrings

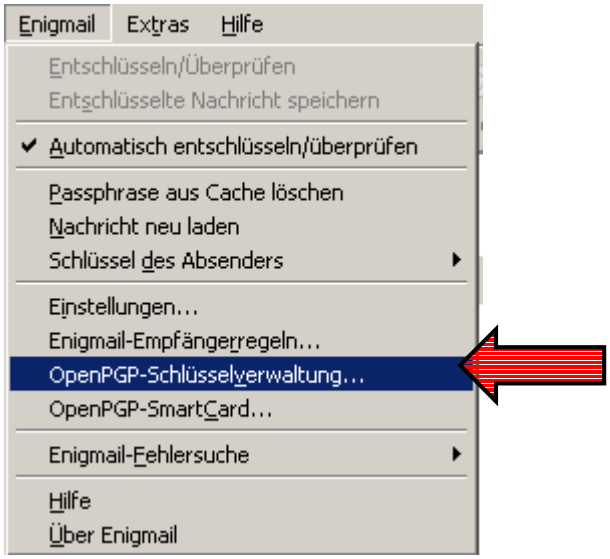
Bevor wir an die Erstellung eines Keyrings (Public Key & Private Key) gehen, ist es ratsam zu prüfen, ob der Pfad zur gpg.exe stimmt. Ist der Pfad nicht korrekt angegeben funktioniert die Schlüssel-Erzeugung nicht. Gehen Sie auf „Konten-Einstellungen bearbeiten“ -> „openPGP-Sicherheit“ -> „Erweitert“ -> Registerreiter „Allgemein“ -> „Pfad zur GnuPG-Anwendung“. Sollte der Pfad nicht korrekt sein, bitte anpassen!



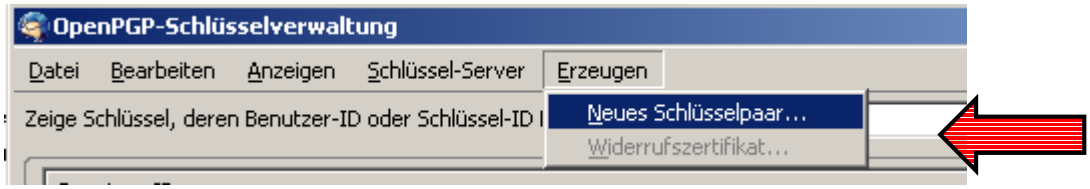
gnu.exe im Installationsverzeichnis auswählen (nur falls Pfad nicht korrekt).



Nach Abschluss der vorangegangenen Arbeitsschritte, geht es jetzt endlich an die Erzeugung des Keyrings. Menü „Enigmail“ -> „OpenPGP-Schlüsselverwaltung“.

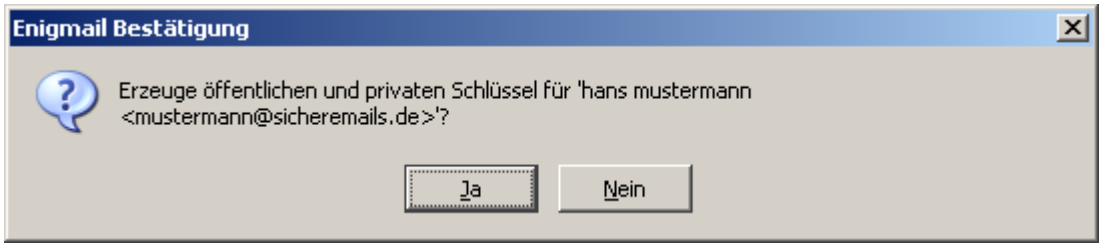


In der Enigmail-Schluesselverwaltung gehen Sie auf „Erzeugen“ -> „Neues Schlüsselpaar“.



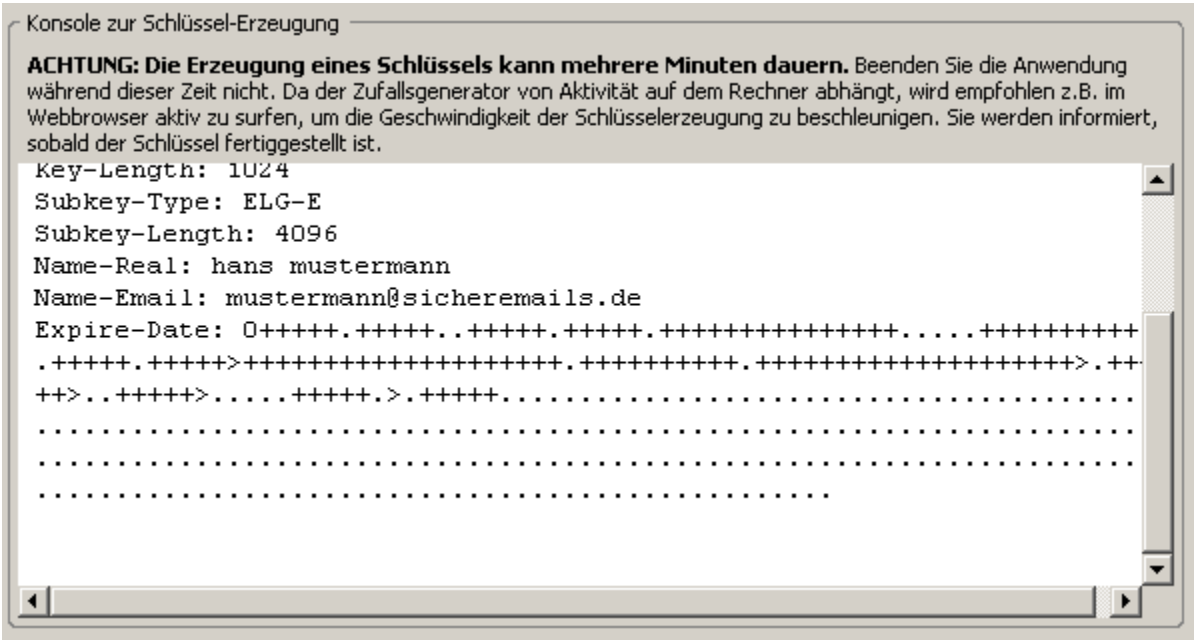
Anschließend klicken Sie auf „Schlüsselpaar erzeugen“

Um den Vorgang abzuschließen und das Schlüsselpaar zu erzeugen bestätigen Sie diese Meldung bitte mit „Ja“.



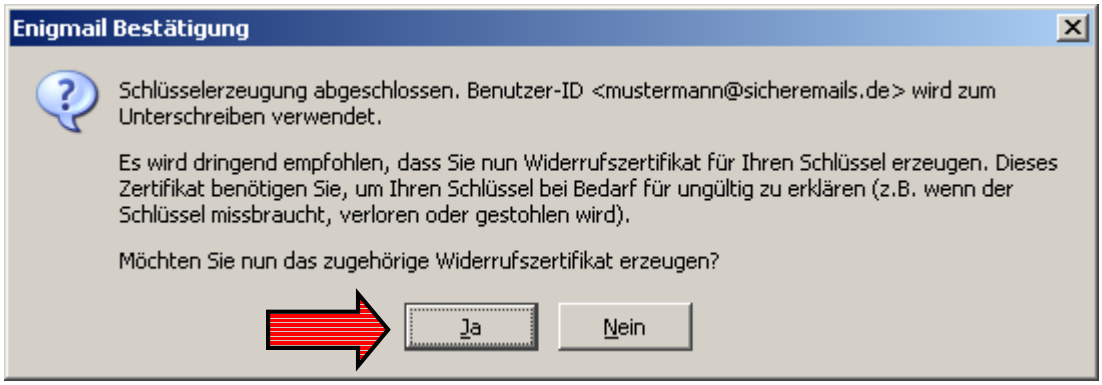
Die Schlüsselerzeugung dauerte auf dem Testrechner (AMD Athlon 1700MHz mit 512 MB SD-RAM) ca. 5 Minuten, wenn Sie nicht gerade ein Power-Rechner oder Dual-Prozessor-System zur Verfügung haben, können Sie in der Zwischenzeit einen Kaffee trinken gehen.

Im Fenster „Konsole zur Schlüssel-Erzeugung“ erscheint jetzt nochmals eine Zusammenfassung der Schlüssel-Eigenschaften (Verschlüsselungs-Algorithmen, Schlüsselstärke usw.). Hinter dem Eintrag „Expire-Date:“ werden laufend Pluszeichen, Punkte etc. dargestellt – dies bedeutet, dass der Prozess der Schlüssel-Erzeugung gerade läuft.

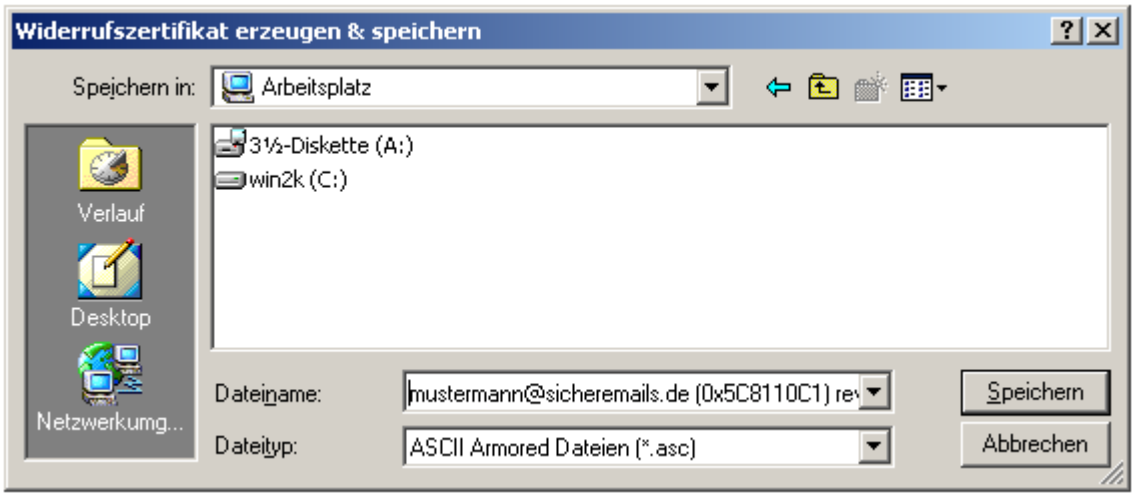


6.2 Erstellung eines Widerrufs-Zertifikats

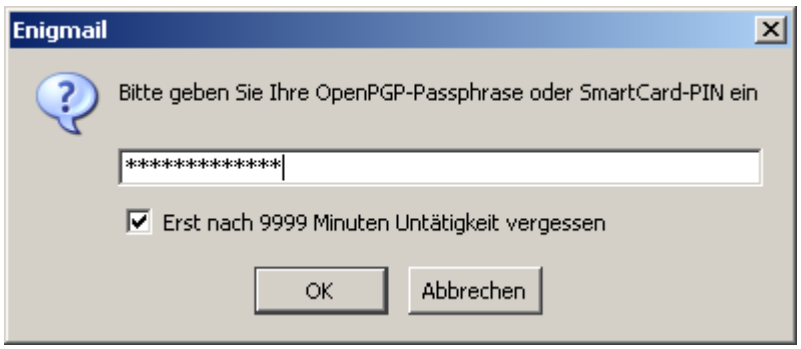
Nachdem das Key Pair erstellt wurde, erscheint eine Erfolgsmeldung.
Des weiteren ist es empfehlenswert ein Widerrufszertifikat (Revokation Key) zu erstellen, falls man seine Passphrase des Privaten Schlüssels vergessen hat, kann man auf diese Weise den Public Key vom Keyserver löschen (ansonsten bleibt der Pub Key für alle Zeiten unwiderruflich auf dem Keyserver!).



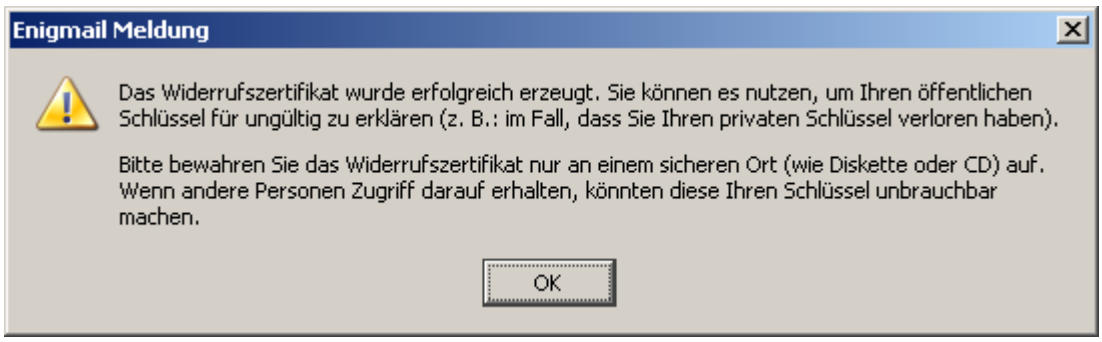
Nach einem Klick auf „Ja“, erscheint ein Fenster in dem Sie den Speicherort für das Widerrufs-Zertifikat auswählen können. Ideal ist es, das Widerrufs-Zertifikat verschlüsselt oder an einem sicheren Ort abzulegen. Wird einer zweiten Person Zugriff auf dieses gewährt, kann er Ihren Public-Key vom Key-Server löschen, dies kann vor allem sehr ärgerlich sein, wenn Sie Ihren Public Key bereits an einen größeren Kontaktkreis weiter gegeben haben.



Abschließend müssen Sie zur Erzeugung des Widerrufs-Zertifikats noch Ihre Passphrase eingeben, ansonsten könnte jeder der Zugriff zu Ihrem Rechner hat ein solches Zertifikat erzeugen!

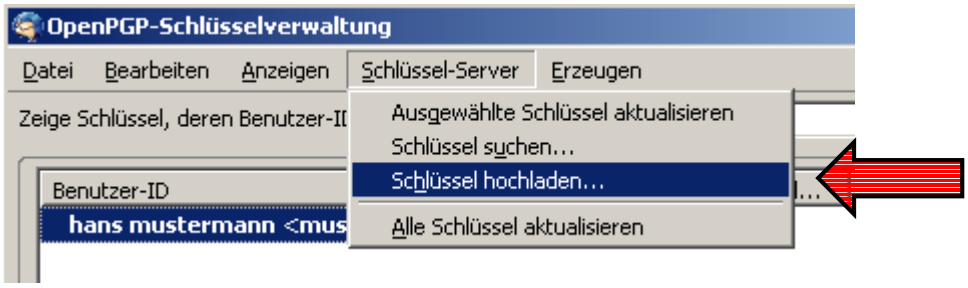


Nach einem Klick auf „OK“ sollte eine Bestätigung erscheinen, in welcher Sie über die erfolgreiche Erstellung des Widerrufs-Zertifikats benachrichtigt werden.



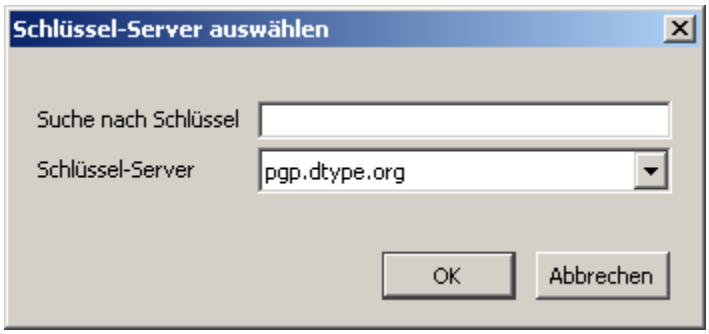
6.3 Public Key auf Keyserver kopieren

Um den Public Key der Öffentlichkeit bekannt zu machen, kann man Ihn innerhalb der OpenPGP-Schlüsselverwaltung auf einen Keyserver kopieren (hochladen).



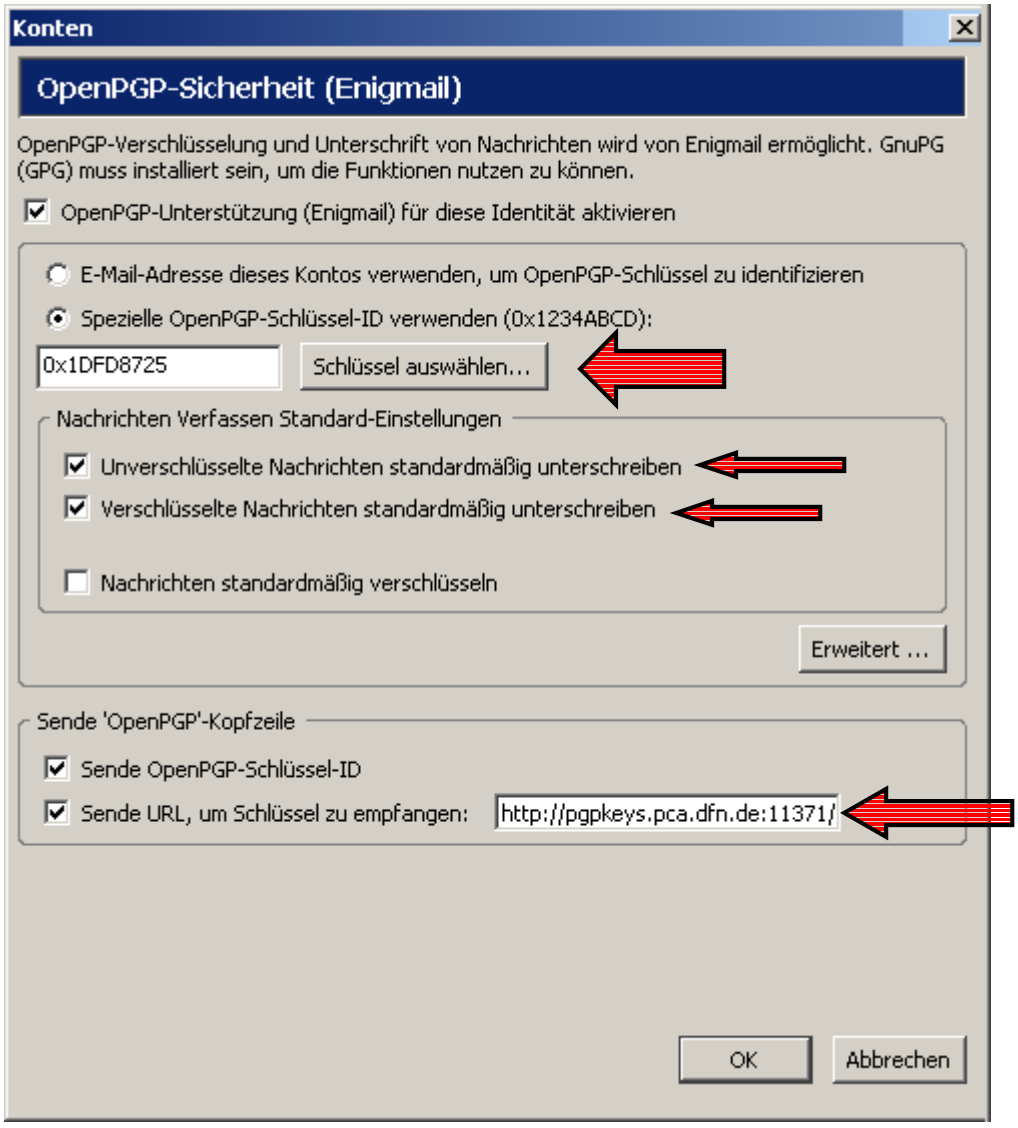
Suchen Sie sich einen Keyserver aus, auf den Sie Ihren Public Key übertragen möchten.

In der Regel spielt dies keine Rolle, da sich die Keyserver untereinander synchronisieren. Bitte beachten Sie, dass dies nicht bei allen Key-Servern der Fall ist. Um auf Nummer sicher zu gehen, ob Ihr Public Key auf den Keyserver XY übertragen wurde, suchen Sie Ihn über die Key-ID -> Menü „Schlüssel-Server“ -> „Schlüssel suchen“. Konnte der Public-Key nicht auf dem Key-Server gefunden werden, können Sie einen erneuten Versuch starten.



Wenn bereits ein Schlüsselpaar erstellt wurde oder Sie bereits eines besitzen, sind sie nur noch einen Katzensprung von der eigentlichen Mail-Signierung/Verschlüsselung entfernt.

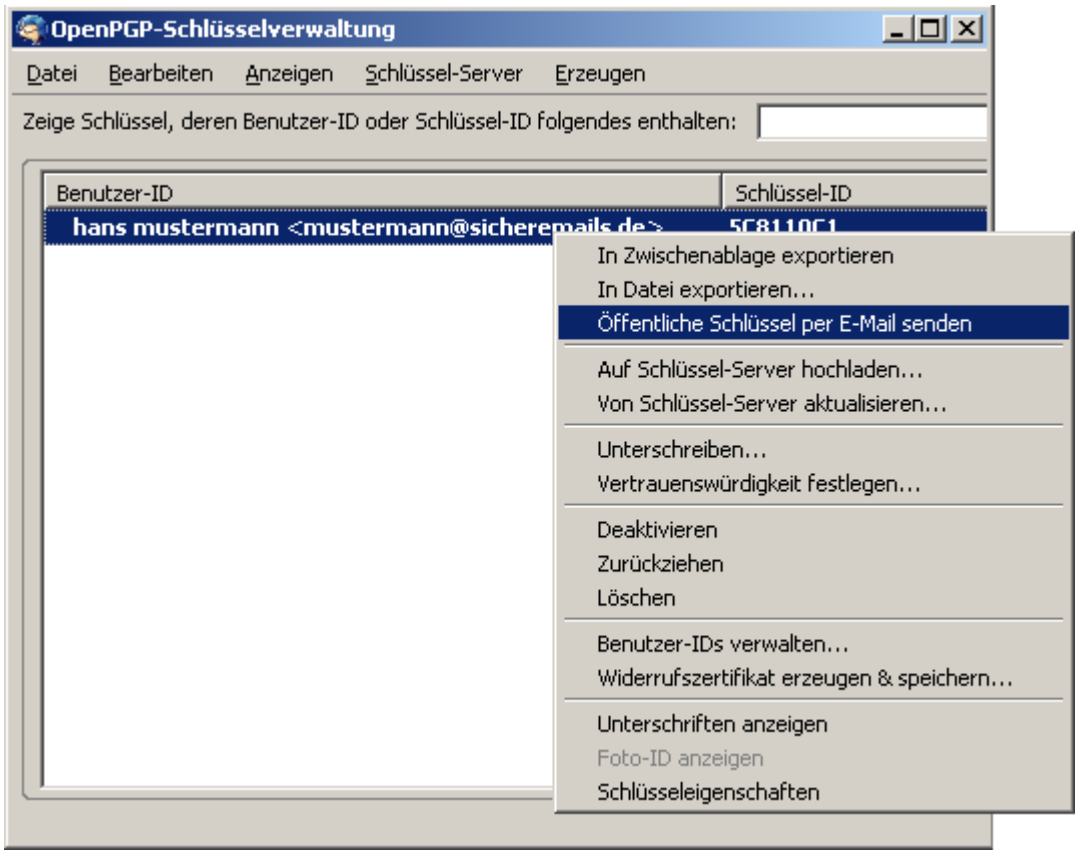
Gehen Sie in die Einstellungen Ihres Mail-Kontos, öffnen Sie dazu folgende Menüpunkte: „Konten-Einstellungen bearbeiten“ -> „OpenPGP-Sicherheit“ Falls Ihr Schlüsselpaar noch nicht ausgewählt ist müssen Sie dies unter „Schlüssel auswählen“ nachholen.



Möchten Sie Ihre Nachrichten standardmäßig verschlüsseln/signieren, so setzten Sie die entsprechenden Haken. In den meisten Fällen ist es ausreichend, eine Mail standardmäßig zu signieren, da man in erster Linie die Identität des Absenders mithilfe der kryptografischen Signatur überprüfen möchte.

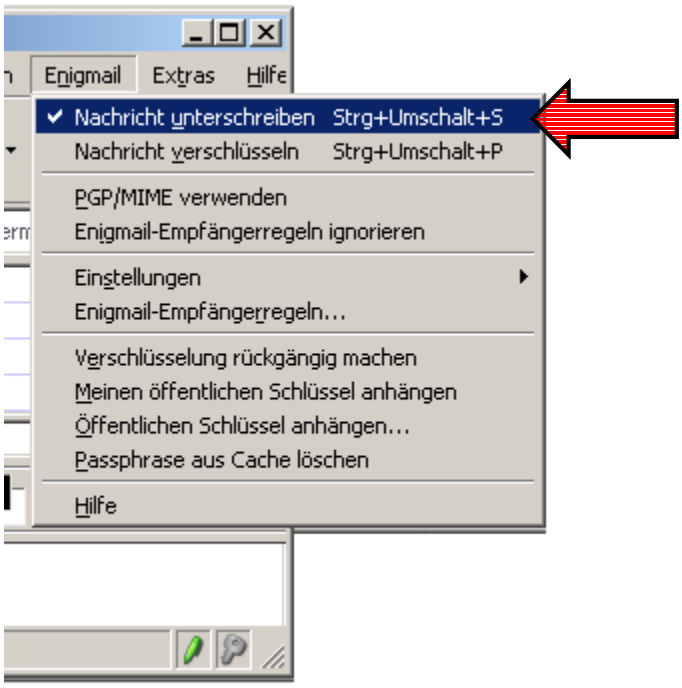
Das Senden der OpenPGP-Schlüssel-ID ist sinnvoll, da der Mailempfänger über diese den Public Key des Mail-Absenders in die OpenPGP-Schlüsselverwaltung importieren kann – hierzu muss allerdings auch der korrekte Pfad des Keyserver eingetragen werden, mit der Key-ID alleine kann „Thunderbird Enigmail“ nichts anfangen.
Eine andere Methode den Public Key dem Empfänger zu überbringen, ist die Möglichkeit ihn per Mail-Anhang als ASCII-Datei zu verschicken:

Hierzu markieren Sie in der OpenPGP-Schlüsselverwaltung Ihren Schlüsselbund, mit einem Rechtsklick gelangen Sie in das Kontextmenü, bitte auf „Öffentliche Schlüssel per E-Mail senden“ klicken.

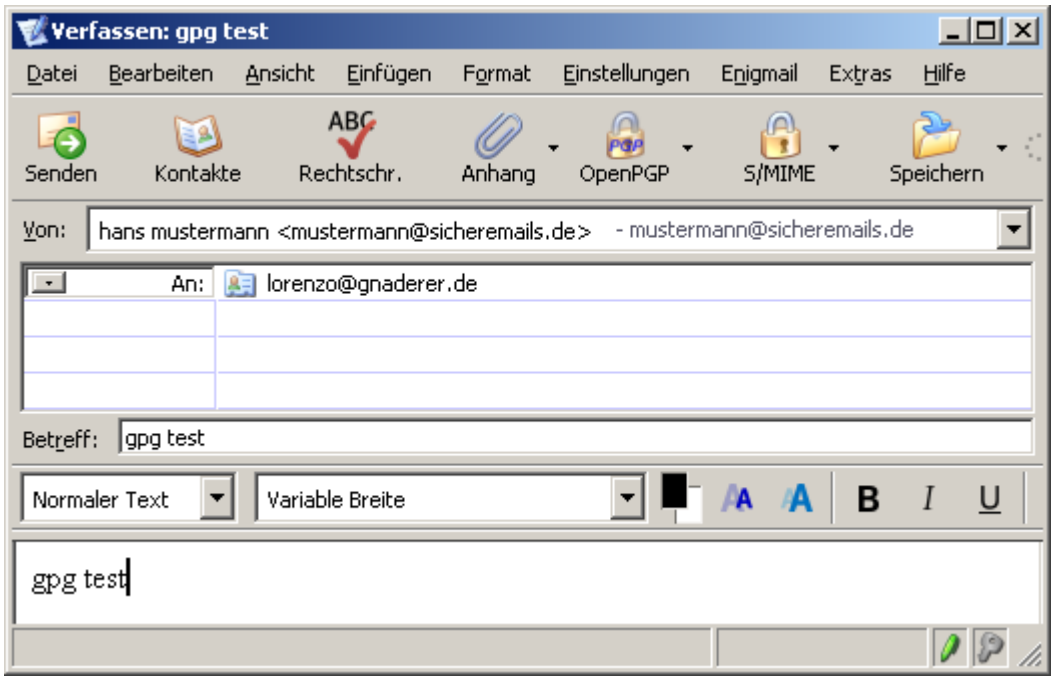


6.4 Mails signieren

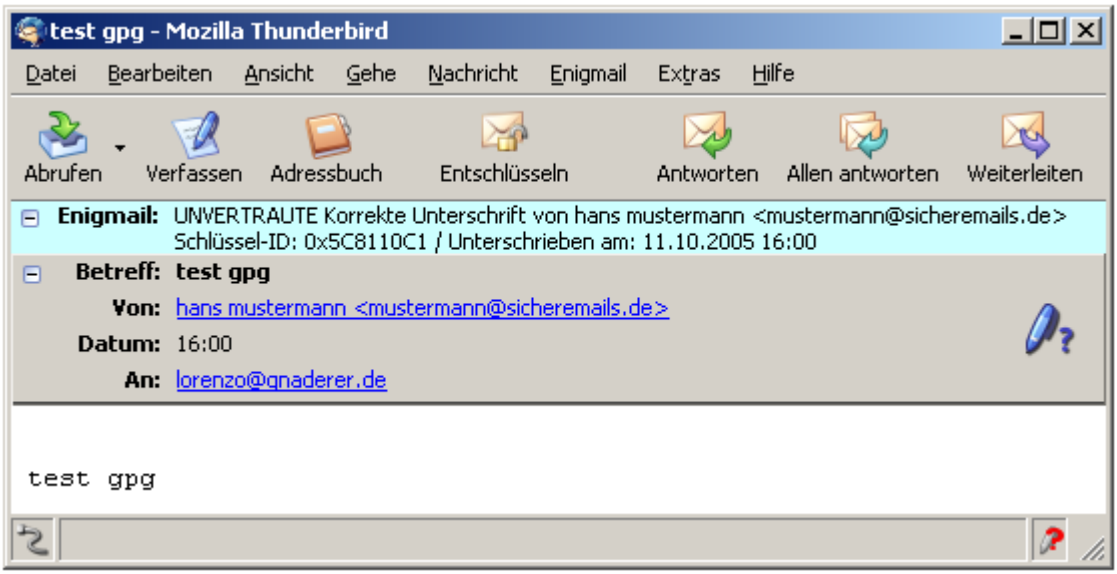
Um eine Mail zu signieren müssen Sie zuerst eine neue öffnen (STRG + N), danach wählen Sie im Menü „Enigmail“ -> „Nachricht unterschreiben“ aus (Haken muss gesetzt sein). Sollten sie Ihre Mails standardmäßig signieren, können Sie diesen Schritt selbstverständlich überspringen.



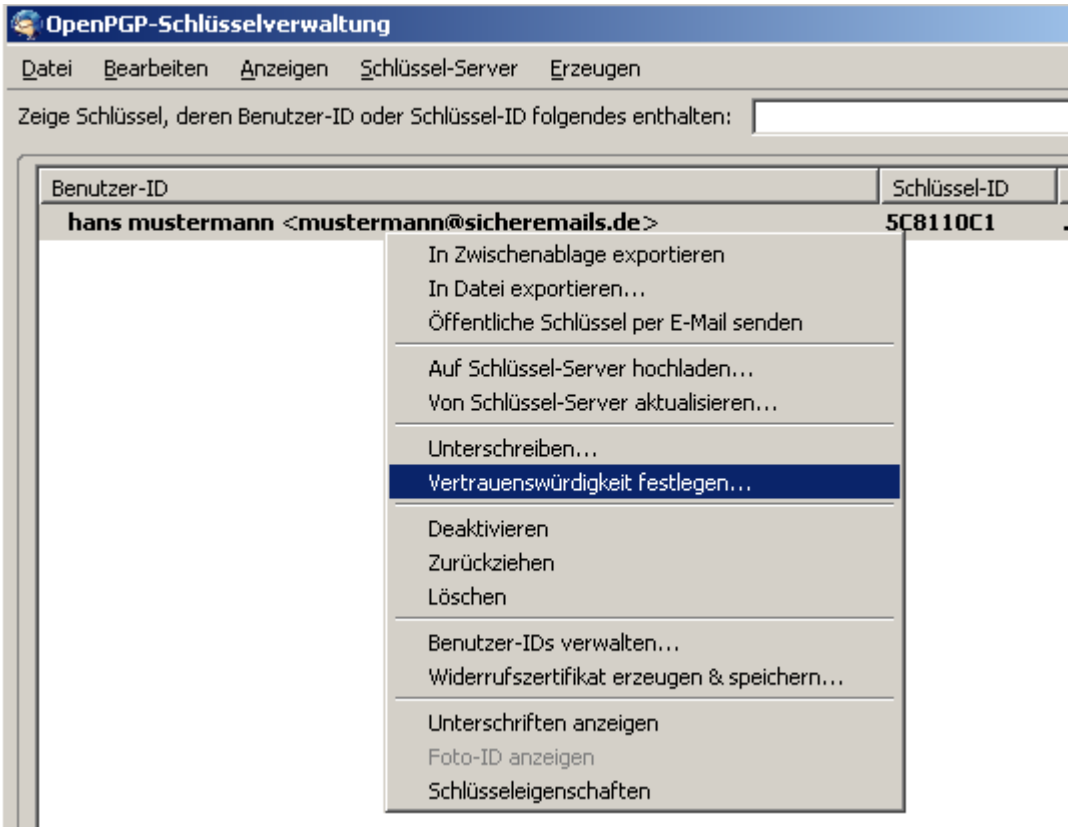
Zu Testzwecken sollte man eine Mail an einen anderen angelegten Mail-Account schicken:



Wenn der Public-Key des Absenders bereits in die OpenPGP-Schlüsselverwaltung eingetragen wurde, kann der Empfänger die signierte/unterschriebene Mail verifizieren (überprüfen). Allerdings erscheint anfangs die Meldung „*UNVERTRAUTE Korrekte Unterschrift von hans mustermann mustermann@sicheremails.de“.* Dies liegt daran, dass dem Public-Key des Mail-Absenders noch nicht vertraut wurde.

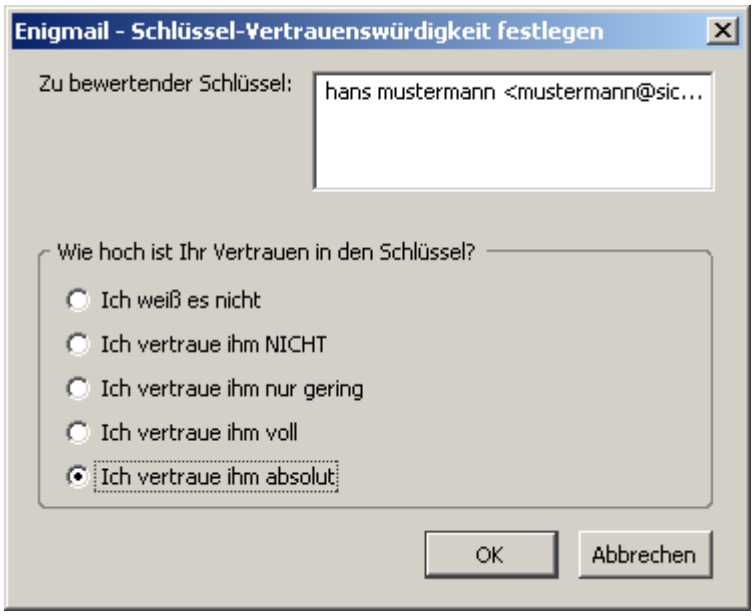


Am besten gehen Sie wieder in die OpenPGP-Schluesselverwaltung um das Vertrauen des importierten Public Key festzulegen.

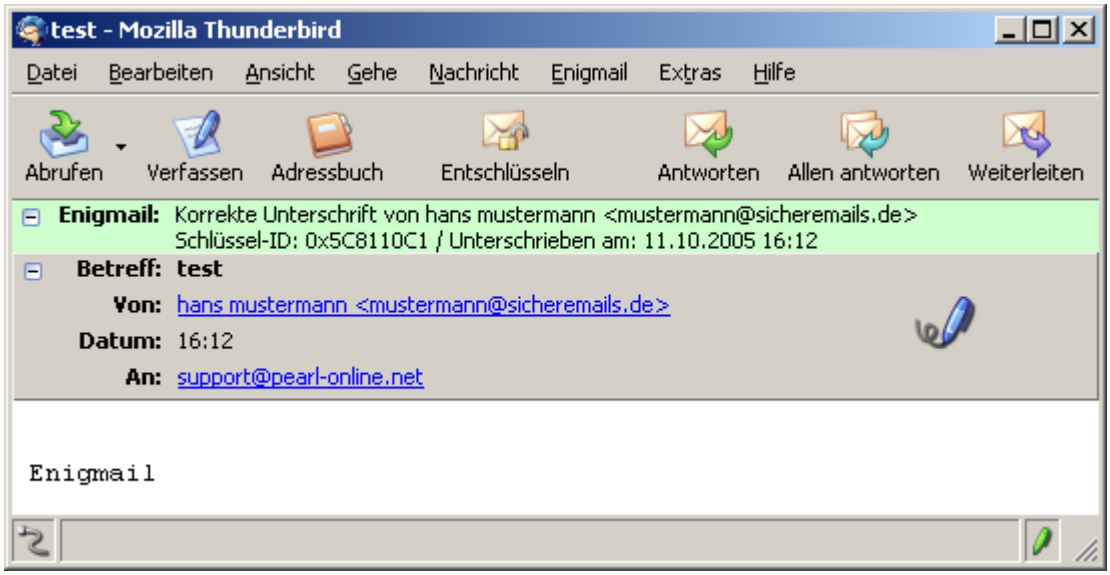


Das Vertrauen muss auf „Ich vertraue ihm absolut“ angehakt werden.

Tun Sie das nur wenn Sie den Fingerprint des Public-Keys (vorzugsweise telefonisch) überprüft haben oder sich absolut sicher sind, dass die Mailadresse der richtigen Person angehört, ansonsten ist die Signatur nutzlos!

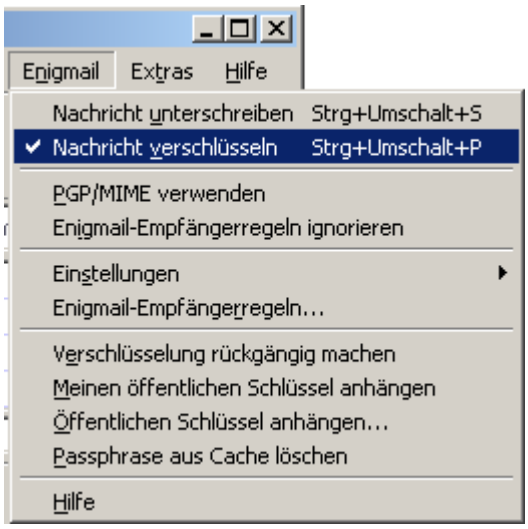


Wurde die Vertrauenswürdigkeit richtig gesetzt, wird jetzt wie gewollt die Meldung „Korrekte Unterschrift von...“ als Enigmail-Kommentar ausgegebenen:

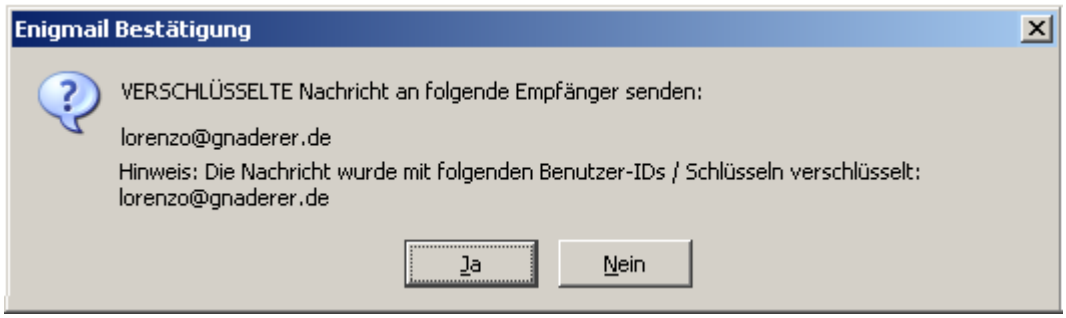


6.5 Mails verschlüsseln

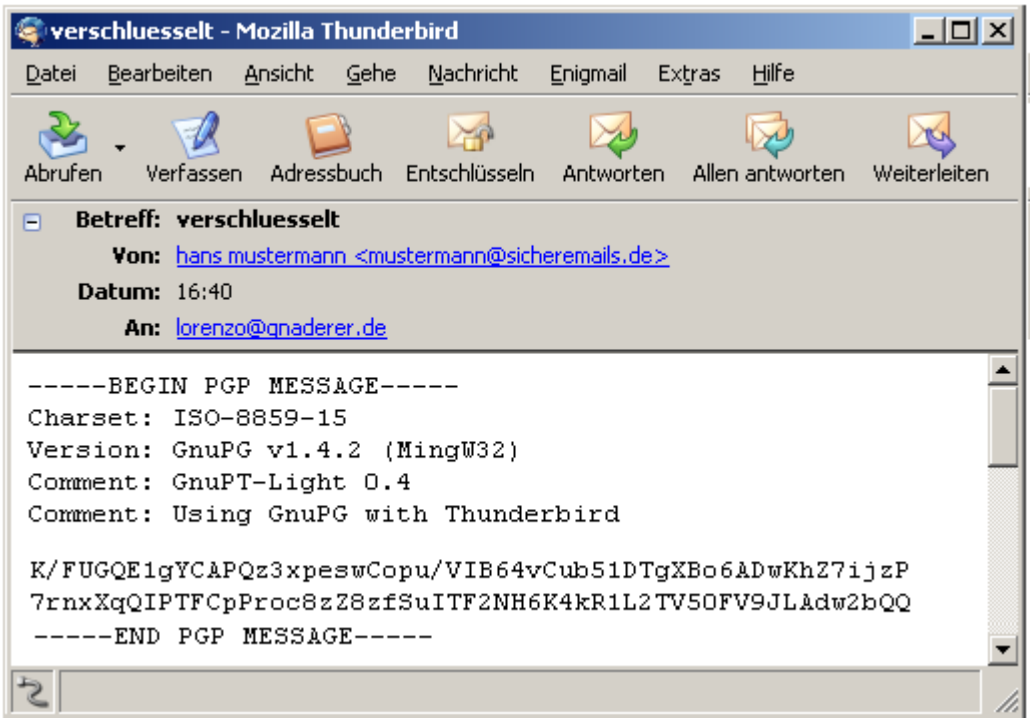
Erstellen Sie zunächst wieder eine neue E-Mail (STRG + N). Anschließend bei „Enigmail“ -> „Nachricht verschlüsseln“ einen Haken setzten.



Bevor die Nachricht verschlüsselt wird, kommt eine Meldung – diese bitte bestätigen:

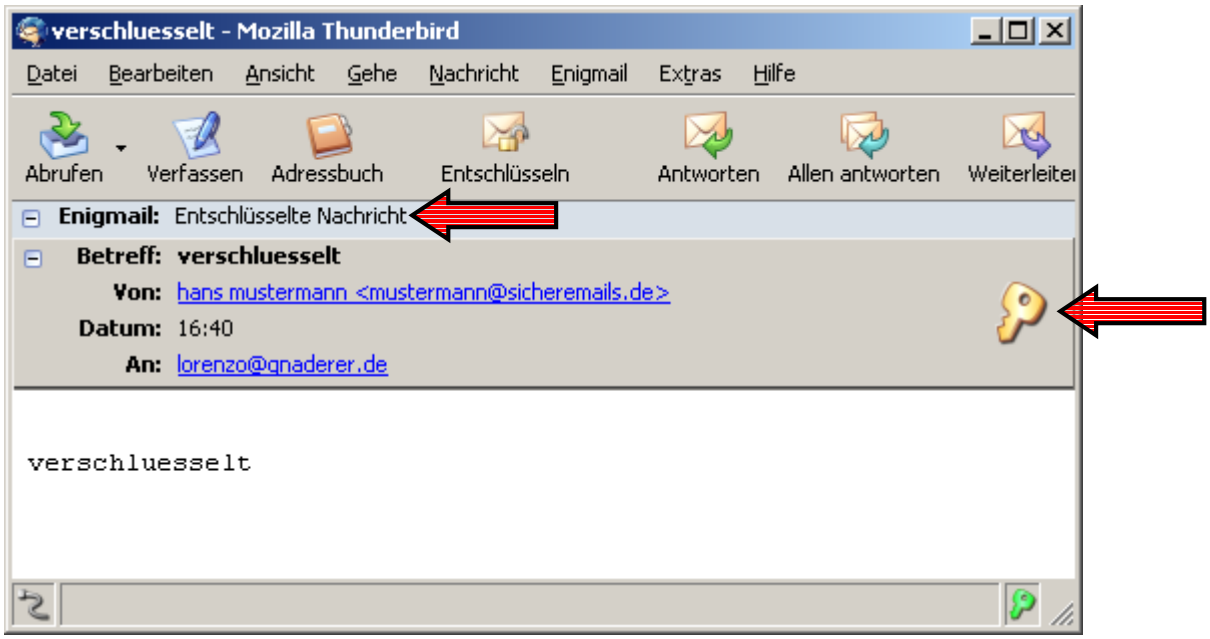


So sieht die Nachricht in verschlüsselter Form aus:



Normalerweise sollte Enigmail die Nachricht automatisch entschlüsseln (mit dem Private Key), ist dies nicht der Fall gehen Sie bitte auf „Enigmail“ -> „Entschlüsseln/Überprüfen“.

Die Nachricht sollte dann im Klartext erscheinen – auch zu erkennen am Schlüsselsymbol und dem Enigmail-Kommentar „Entschlüsselte Nachricht“:



So sieht eine E-Mail aus die sowohl verifiziert (Signatur) als auch entschlüsselt wurde:

Hat alles geklappt wird ein „Kugelschreibersymbol“ und ein „Schloss“ angezeigt, ein grün hinterlegtes Enigmail-Kommentar, wie in der Abbildung zu sehen ist, gibt die Erfolgs-Bestätigung nochmals in Text-Form aus.

7 Quellenangeben

7.1 Print-Medien

- Internet-Sicherheit für Einsteiger von Alexander Otto (Galileo Computing)

7.2 Internet

- www.google.de
- www.wikipedia.de
- http://kai.iks-jena.de/pgp/gpg/
- Einführung in die Kryptographie von Network Associates

7.3 Grafiken

- Grafiken zur Signierung von Network Associates