

Provisorisch

## Handbuch für Gnu-Privacy Guard für Windows

Stand 10.05.2007

Haftung wird weder für die Richtigkeit  
noch für die Qualität der Software übernommen.

***pb***

## 1. **Einleitung**

- 1.1. Für NGOs ( privatwirtschaftliche Organisationen ) sind die Vereinbarungen, die notwendig sind, um Sicherheit in der Weltnetz-Kommunikation zu gewährleisten, schwer zu erreichen. Für Regierungen und Firmen ist es wesentlich leichter: Man hat i.d.R. eine EDV-Abteilung und das notwendige Mittel für die Beschaffung der erforderlichen Hard-, Software sowie Vorgehensweisen. Organisatorisch gesehen, ist es auch für NGOs mit Schwierigkeiten verbunden, weil Aufsicht und Arbeitsverfolgung fehlt.
- 1.2. Dank der Arbeit der Firma **Intevation GmbH**, Osnabruck (<http://www.intevation.net>) können mindestens einige der Nachteile für die NGOs überwunden werden. Sie haben ein Produkt GPG4Win unter dem **GNU public Licence** ( <http://www.gnu.org>) auf dem Markt gebracht. Zusammen mit dem Produkt der **Mozilla Corporation** (<http://www.mozilla.com/en-US/about/contact.html>) **Thunderbird E-Mail Client** ist es nunmehr möglich, ein Gesamtpakte von professioneller Software für NGOs für den Austausch verschlüsselter E-Mails zur Verfügung zu stellen.
- 1.3. Was die Verwendung von Thunderbird angeht, **empfehlen wir eine separate E-Mail Adresse für verschlüsselte E-Mails anzulegen**. Dies macht die versehentliche Sendung von Klartext-Mails weniger wahrscheinlich. Es ist insbesondere nötig, wo andere E-Mail Clients verwendet werden.

## **2. Installation von GnuPG**

2.1. Am besten hält man nachfolgende Installationsreihenfolge ein.

GPG for Windows "gpg4Win" Version 1.1.0.

„Thunderbird“ 2.0 E-Mail-Klient

„Enigmail“, Plug-in für Thunderbird Version .

2.2. Dieses Handbuch wurde für Windows XP geschrieben. Andere Windows Systeme werden ähnliche Dialoge zeigen sein. Etwa 50 MB freier Speicherkapazität wird benötigt bei einer Taktfrequenz von mehr als 400 MHz

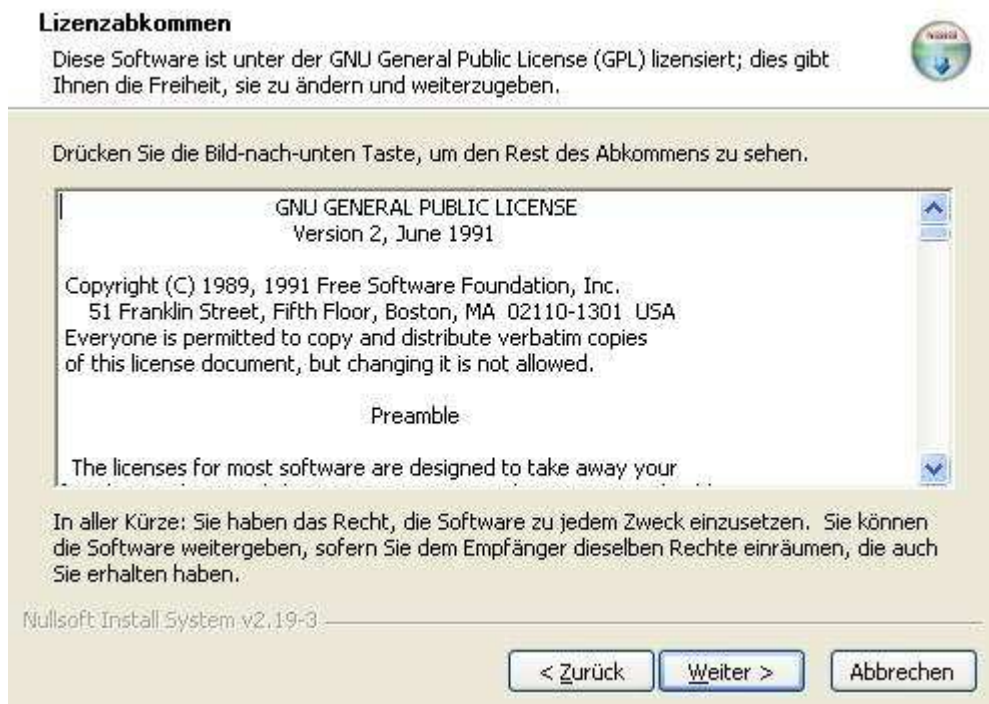
2.3. Der Software wird vertraut, weil die Quellcodes zur Verfügung gestellt werden.

### 3. GPG for Windows

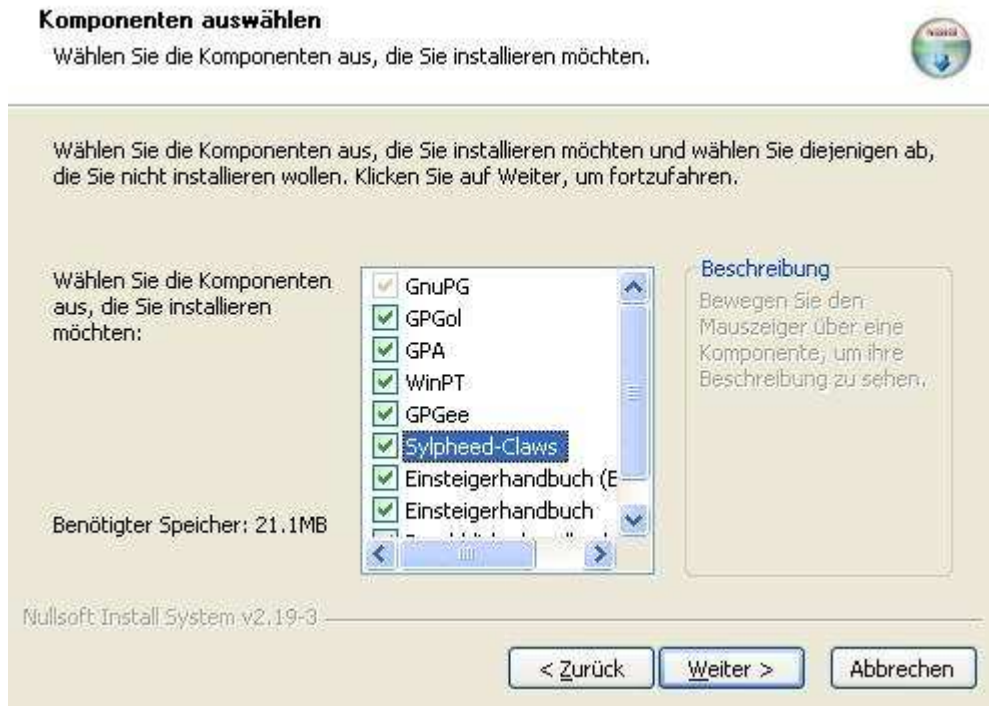
- 3.1. Start **gpg4win-1.0.0.exe** mit einem Doppelklick. Falls Sie Erfahrung haben dann können Sie dieses Kapitel ausklammern und GPG for Windows wie normal installieren. Ansonsten unmittelbar nach dem Doppelklick sehen Sie untenstehende Meldung. Klicken Sie auf "**weiter**".



- 3.2. Sie werden dann die Lizenz-Vereinbarung. Lesen Sie dies und Klicken Sie auf "**weiter**".



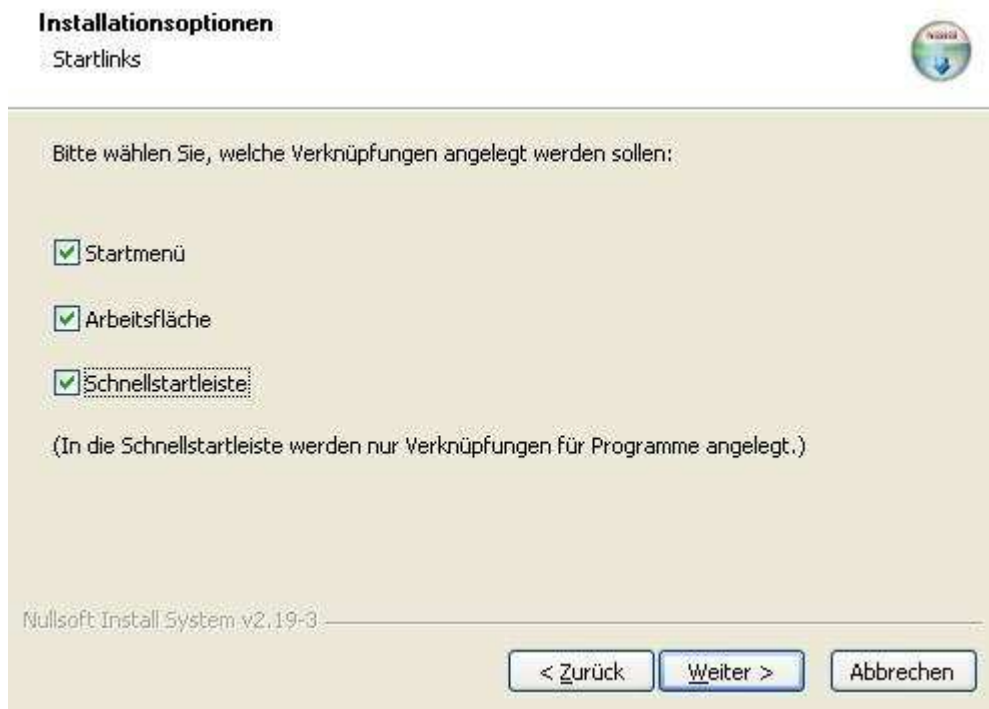
- 3.3. Sie erhalten eine Auswahl-Menu. Wählen Sie mindestens die bereits angekreuzten. Dann klicken Sie "**Weiter**".



- 3.4. Sie bekommen einen Vorschlag zum Installationspfad. Akzeptieren Sie diesen, es sei denn, Sie haben gute Gründe den zu ändern. Klicken Sie auf "**Weiter**".



- 3.5. Die Start-Links auswählen. Vorschlag, mindestens die "**Startmenu**". Klicken Sie "**Weiter**".



- 3.6. Klicken Sie "**Installieren**"



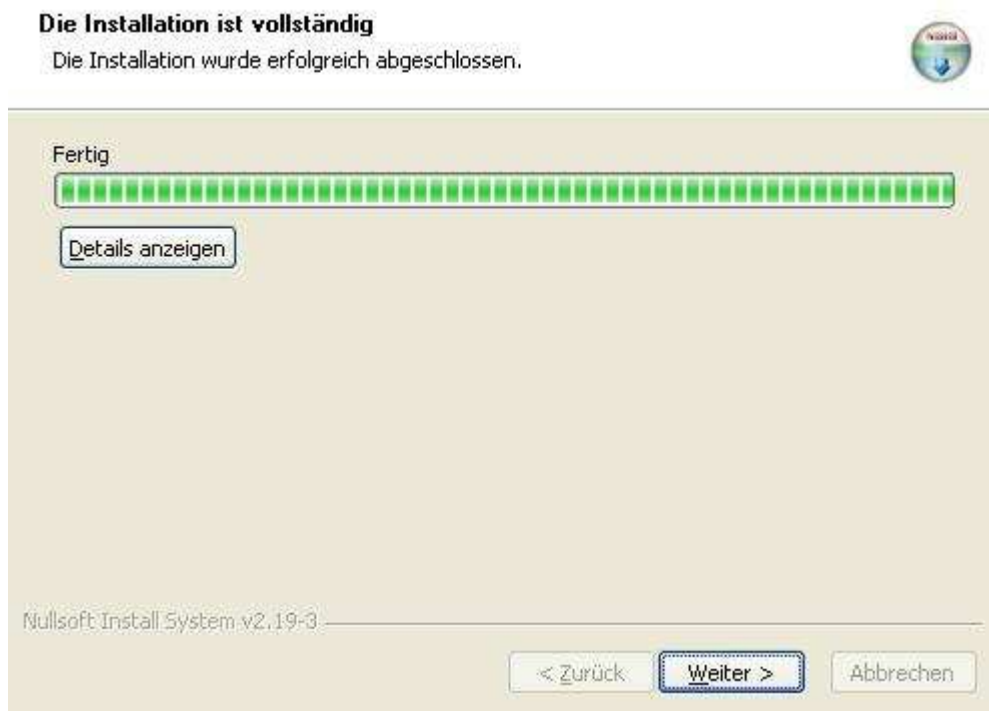
### 3.7. Die Installation beginnt:



### 3.8. Kann sein, dass Sie folgende Meldung erhalten. Klicken Sie "OK" und ignorieren Sie es.



3.9. Die Installation geht zu Ende. Klicken Sie auf "**Weiter**".



3.10. Der Abschluss:



3.11. Fertig. Sie brauchen für GPG 4 Win nicht mehr zu machen. Glückwunsch !

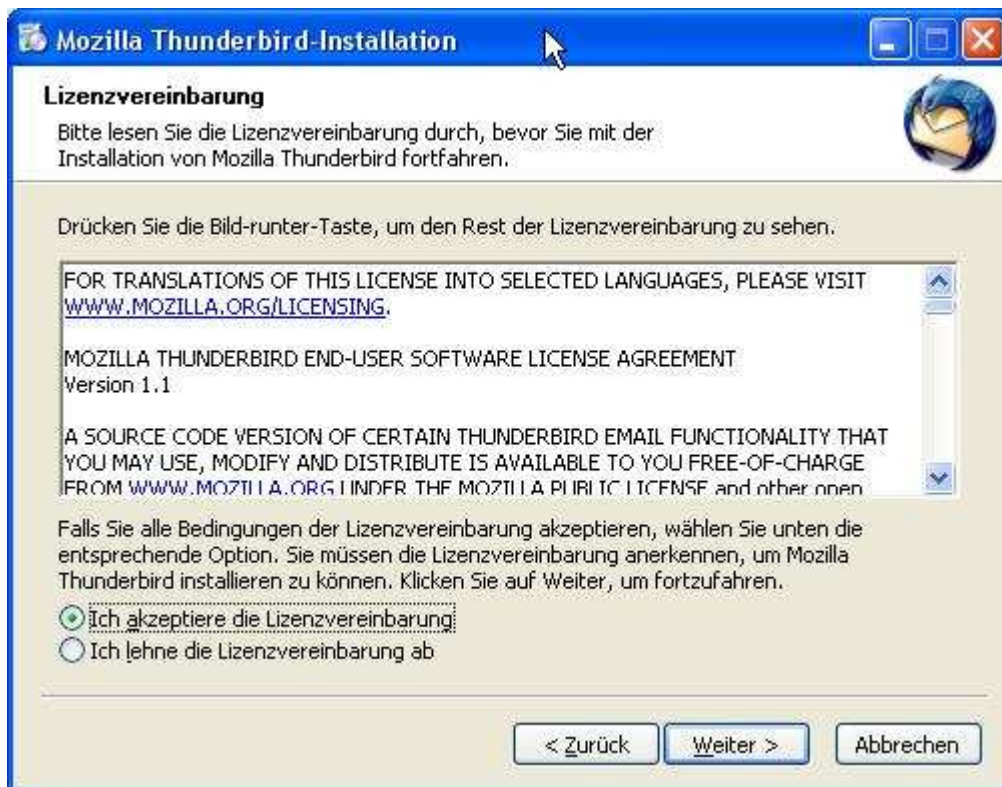
#### 4. **Installation von Thunderbird 2.**

- 4.1. Falls Sie Thunderbird nicht bereits installiert haben. Dann doppelklicken Sie auf "**Thunderbird2.exe**"

Sie sehen dann: Klicken Sie "**Weiter**".



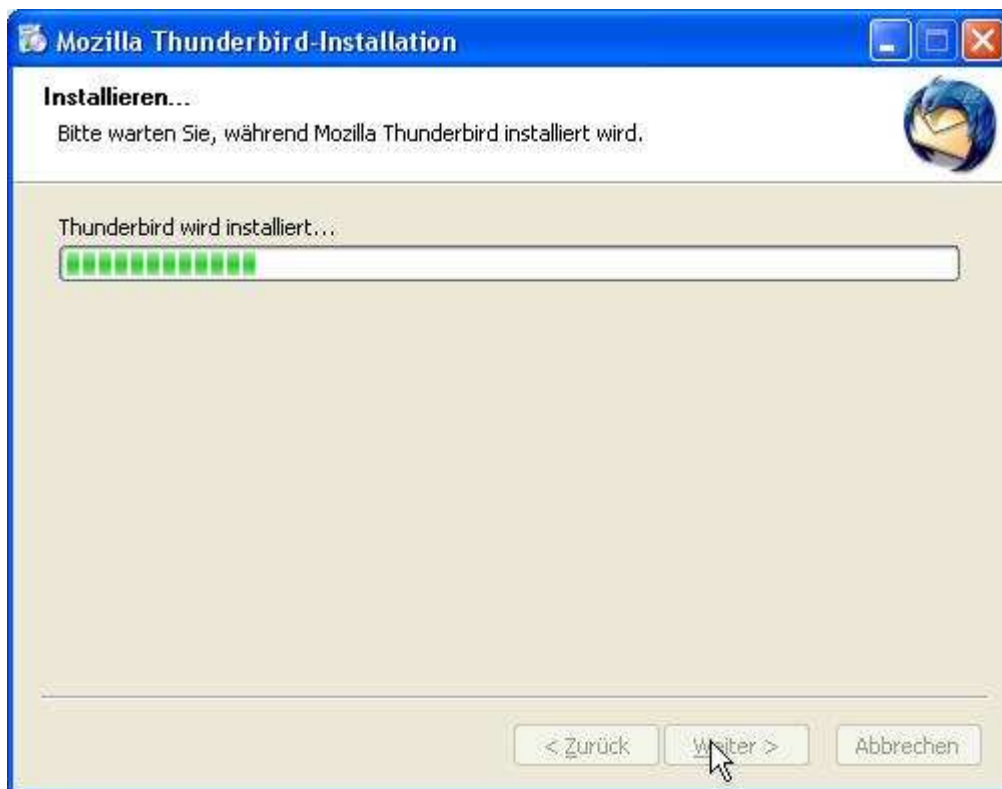
- 4.2. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie sie und Klicken Sie **"Weiter"**.



- 4.3. Wählen Sie Standard und klicken Sie **"Weiter"**.



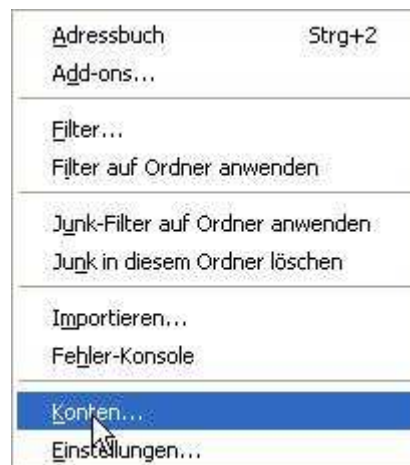
4.4. Die Installation beginnt:



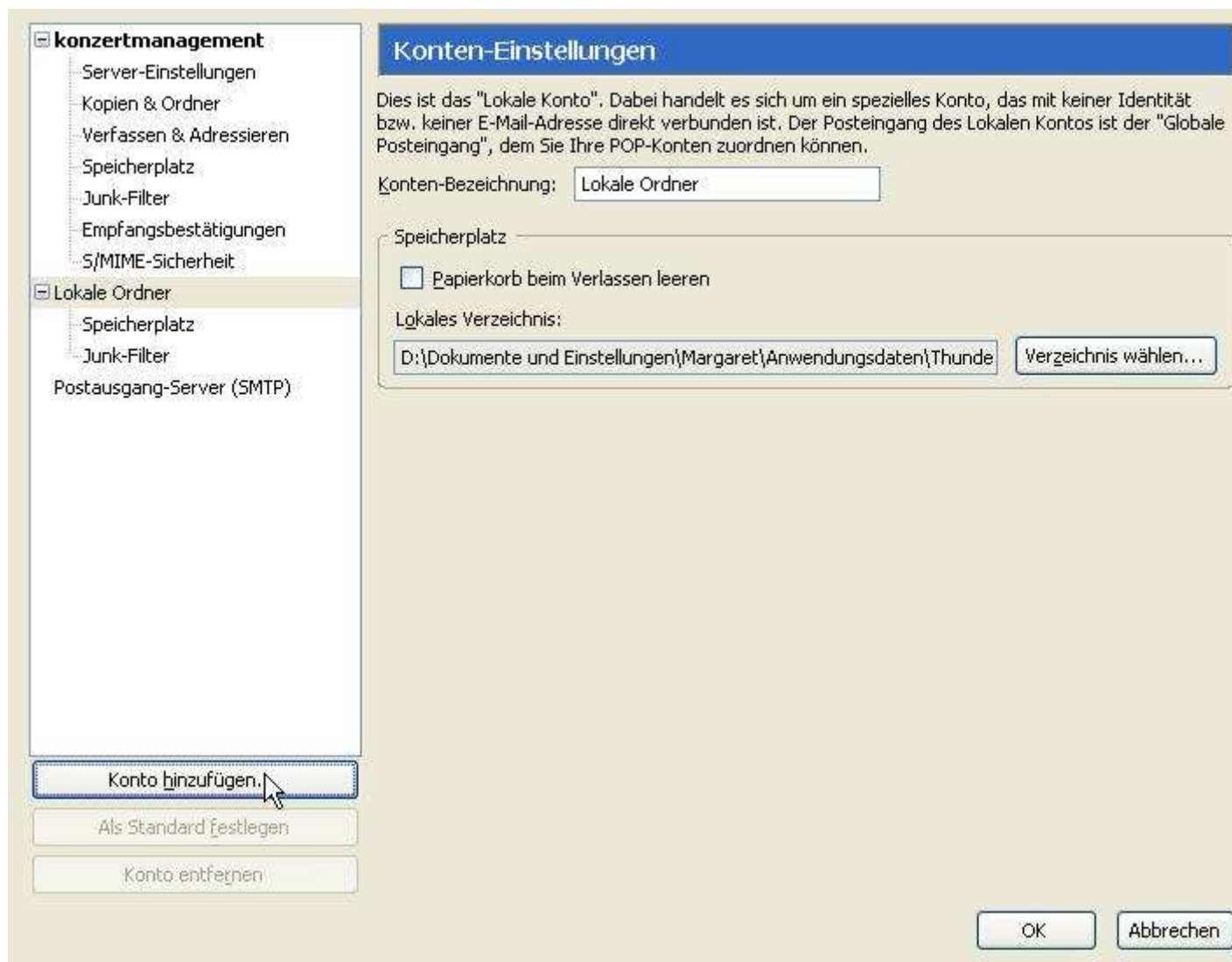
4.5. Die Installation geht zu Ende. Klicken Sie auf Fertigstellen:



4.6. Klicken Sie auf Extras um ein Email-Konto einzustellen:




4.7. Sie sehen dann. Wählen Sie "Konto hinzufügen".



#### 4.8. Wählen Sie "E-mail-Konto":

Um Nachrichten empfangen zu können, müssen Sie zuerst ein Konto anlegen.  
Dieser Assistent sammelt Informationen, die notwendig sind, um ein neues Konto einzurichten.  
Wenn Sie die abgefragten Daten nicht kennen, kontaktieren Sie bitte Ihren Systemadministrator oder Internet Service Provider.  
Wählen Sie den Konten-Typ, den Sie einrichten möchten:

- E-Mail-Konto
- RSS-Konto
- Google Mail
- Newsgruppen-Konto



- 4.9. Tragen Sie Ihren Namen und E-Mail-Adresse ein. **Hier ist es ratsam, eine separate E-Mail-Adresse für verschlüsselte Mails zu bestellen. Falls Sie nicht selber über mehrfache E-Mails verfügen, dann gibt es Providers von kostenlosen Adressen, z.B. Google Mail oder GMX. Dies macht Fehler, z.B. das versehentliche Senden von Klartext, weniger wahrscheinlich. Falls Sie ansonsten 'Thunderbird' nicht benutzen, dann ist eine separate Adresse ein muss.**

#### Identität

Diese Informationen erhalten Empfänger Ihrer Nachrichten.

Geben Sie den Namen an, der im Feld "Von" Ihrer gesendeten Nachrichten erscheinen soll (zum Beispiel "Hermann Maier").

Ihr Name:

Geben Sie Ihre E-Mail-Adresse an. Diese Adresse ist jene, die andere verwenden, um Ihnen Nachrichten zu senden (zum Beispiel "benutzer@beispiel.de").

E-Mail-Adresse:

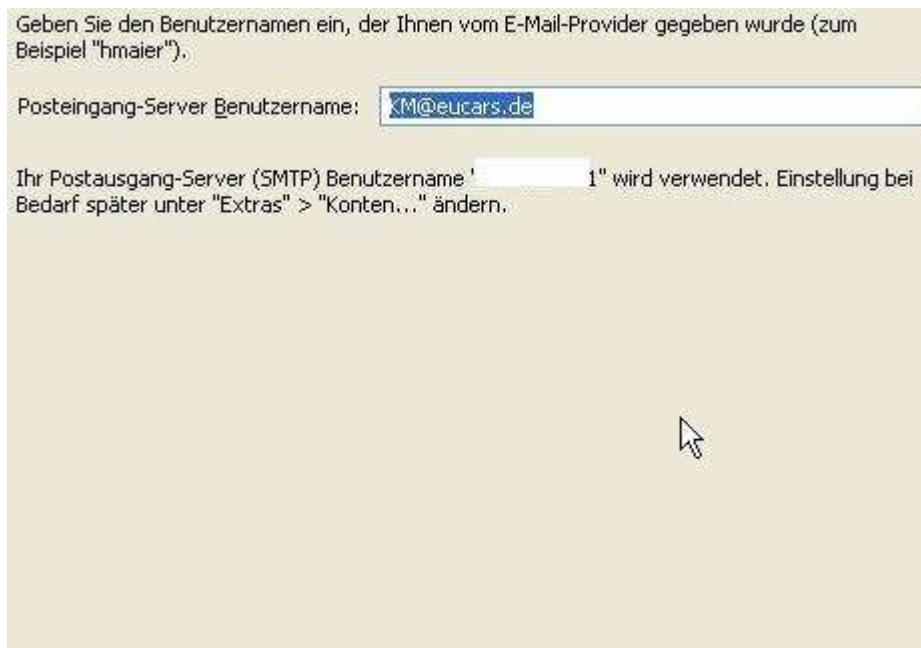
< Zurück Weiter > Abbrechen

- 4.10. Tragen Sie den Benutzernamen, den Ihr Provider bestimmt hat, hier ein. Der Benutzername kann Ihre E-Mail-Adresse sein, muss aber nicht:

Geben Sie den Benutzernamen ein, der Ihnen vom E-Mail-Provider gegeben wurde (zum Beispiel "hmaier").

Posteingang-Server Benutzername:

Ihr Postausgang-Server (SMTP) Benutzername '  1' wird verwendet. Einstellung bei Bedarf später unter "Extras" > "Konten..." ändern.



- 4.11. Die Kontenbezeichnung ist informell.

Geben Sie eine Bezeichnung für das Konto ein, mit der das Konto im Programm erscheinen soll (zum Beispiel "Arbeits-Konto", "Privat-Konto" oder "News-Konto").

Konten-Bezeichnung:



- 4.12. Jetzt bekommen Sie die Daten, die Sie eingetragen haben zusammengefasst. Drücken Sie auf "**Fertigstellen**" oder "**Zurück**", um evtl. Fehler zu korrigieren.

### Zusammenfassung

Bitte prüfen Sie, ob die Angaben korrekt sind:

Konten-Bezeichnung:	KM
E-Mail-Adresse:	KM@eucars.de
Posteingang-Server Benutzername:	KM@eucars.de
Posteingang-Server:	pop.1und1.de
Typ des Posteingang-Server:	POP3
Postausgang-Server (SMTP) Benutzername:	<input type="text"/>
Postausgang-Server (SMTP):	smtp.1und1.de

Klicken Sie "Fertig stellen", um diese Einstellungen zu speichern und den Konten-Assistenten zu beenden.

- 4.13. Falls sie die Out-Sever einstellen müssen ( weil z.B. Sie eine andere Provider haben oder Sie mache es zum ersten mal ) , dann drücken Sie im Hauptdialog auf "Postausgang-Server (SMTP)" - ganz links und Sie bekommen:

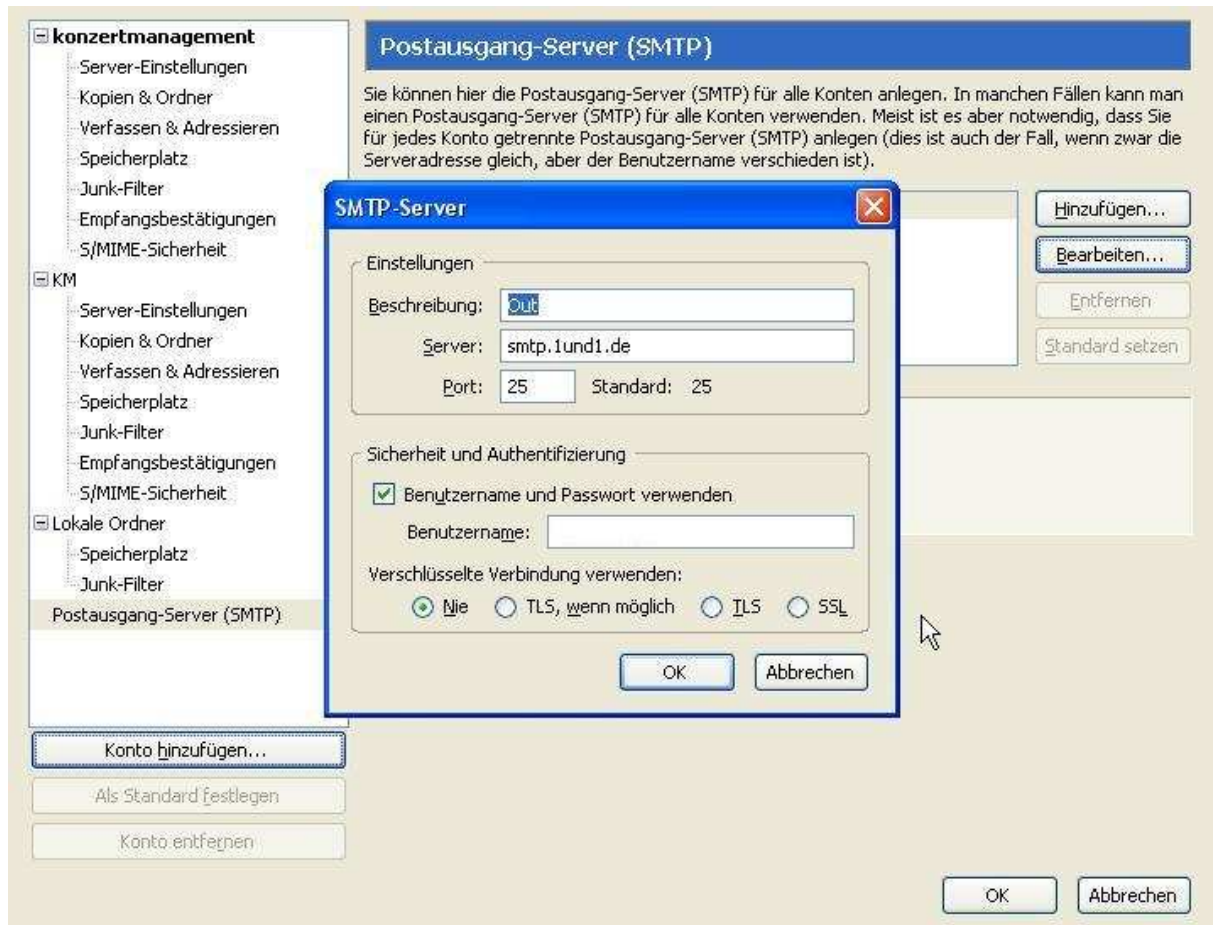
**Postausgang-Server (SMTP)**

Sie können hier die Postausgang-Server (SMTP) für alle Konten anlegen. In manchen Fällen kann man einen Postausgang-Server (SMTP) für alle Konten verwenden. Meist ist es aber notwendig, dass Sie für jedes Konto getrennte Postausgang-Server (SMTP) anlegen (dies ist auch der Fall, wenn zwar die Serveradresse gleich, aber der Benutzername verschieden ist).

Out - smtp.1und1.de (Standard)	Hinzufügen...
	Bearbeiten...
	Entfernen
	Standard setzen

Beschreibung: Out  
Server: smtp.1und1.de  
Port: 25  
Benutzername:   
Sichere Verbindung:  Nein

- 4.14. Sie bekommen einen Dialog zur Eintragung der SMTP (Out-Server) -Daten die Sie bitte von Ihrem Provider beziehen. Sie können das Passwort hinter dem Benutzernamen getrennt durch einen "#" eingeben. Dies wird allerdings nicht empfohlen, weil dann jeder, der am Computer sitzt, es sehen kann. Falls Sie es nicht eingeben, dann werden sie in der Anwendung danach gefragt und sie können es geschützt eingeben, wie ein normales Passwort,



## 5. Der Einigmail Plug-in

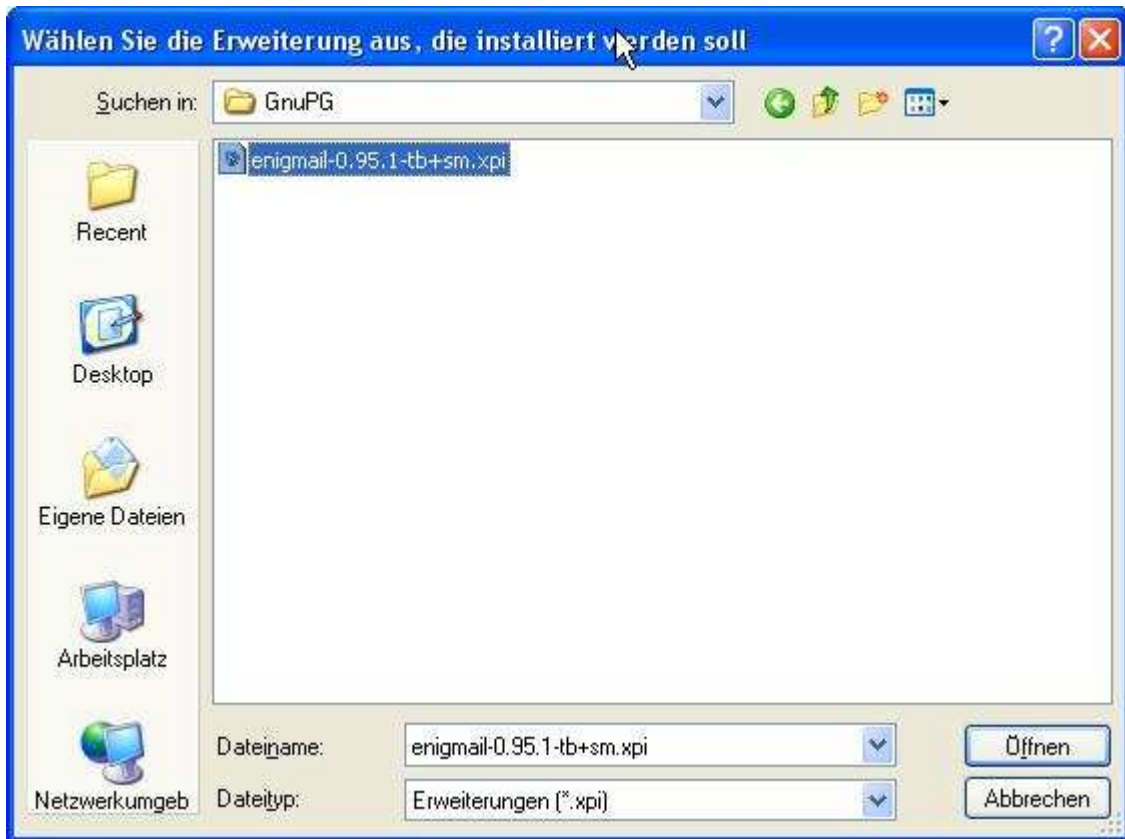
5.1. Jetzt wird der notwendige Plug-In installiert. Wählen Sie "Extras" und "Add-ons":



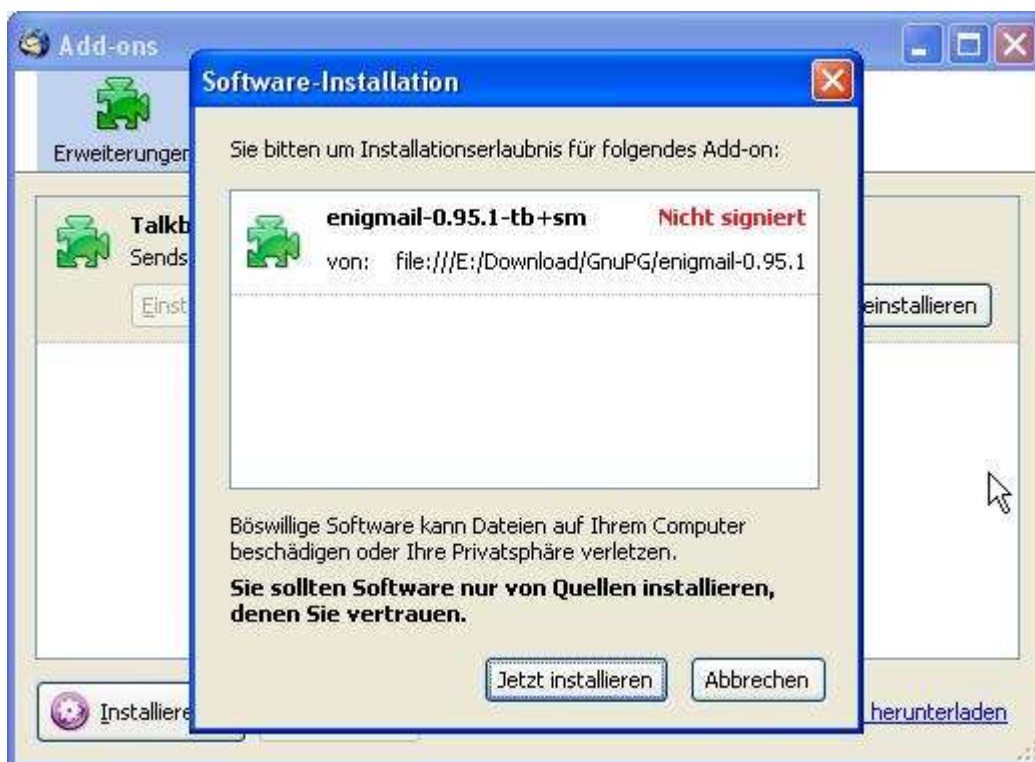
5.2. Sie bekommen einen Dialog. Drücken Sie auf "Installieren".



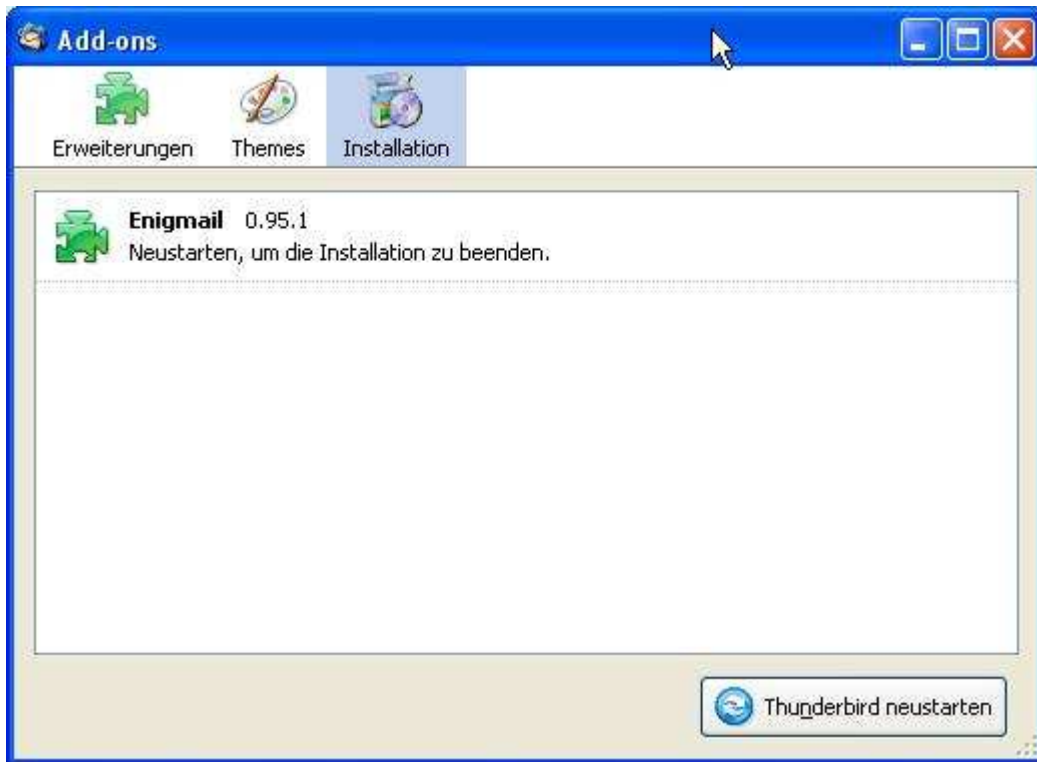
- 5.3. Sie bekommen den Datei-Suchdialog. Suchen Sie die Add-on "enigmail-0.95.1+sm.xpl", die Sie vorhin bereits heruntergeladen haben.



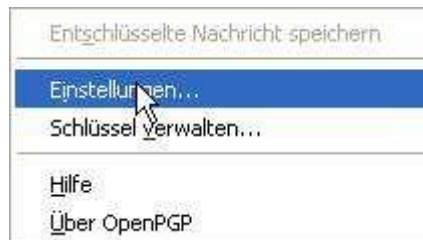
- 5.4. Drücken Sie auf "Öffnen". Sie sehen dann den untenstehenden Dialog. Drücken Sie auf "Installieren".



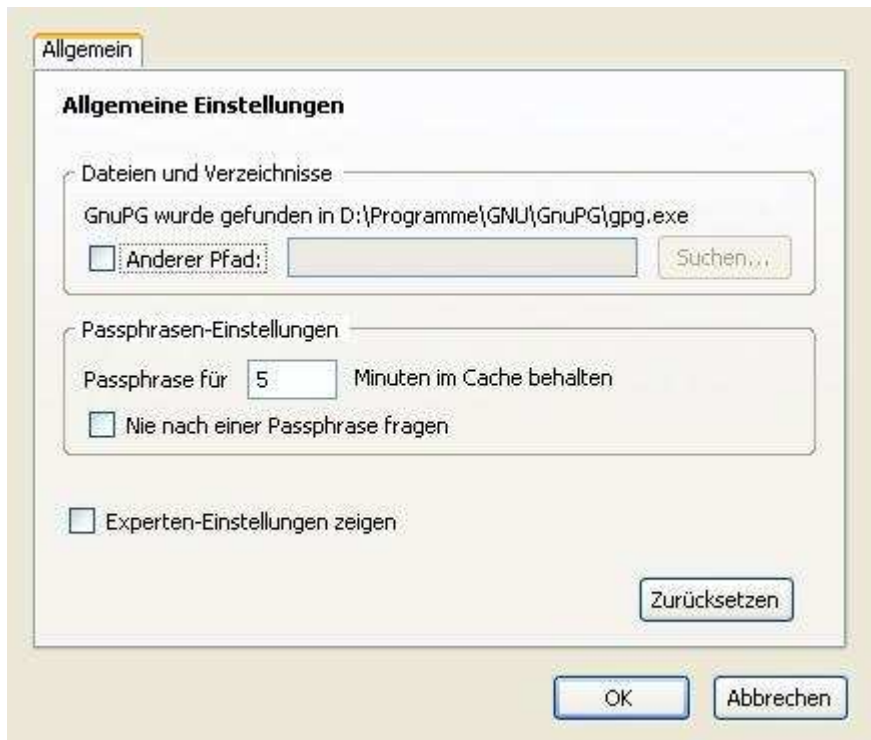
- 5.5. Sie sehen dann einen Dialog, der Sie informiert, dass Thunderbird neu gestartet wird.



- 5.6. Wenn Thunderbird neu startet und Sie sehen einen neuen Menu "OpenPGP" haben Sie den Plug-in erfolgreich installiert. Öffnen Sie die "Einstellungen" unter "OpenPGP"



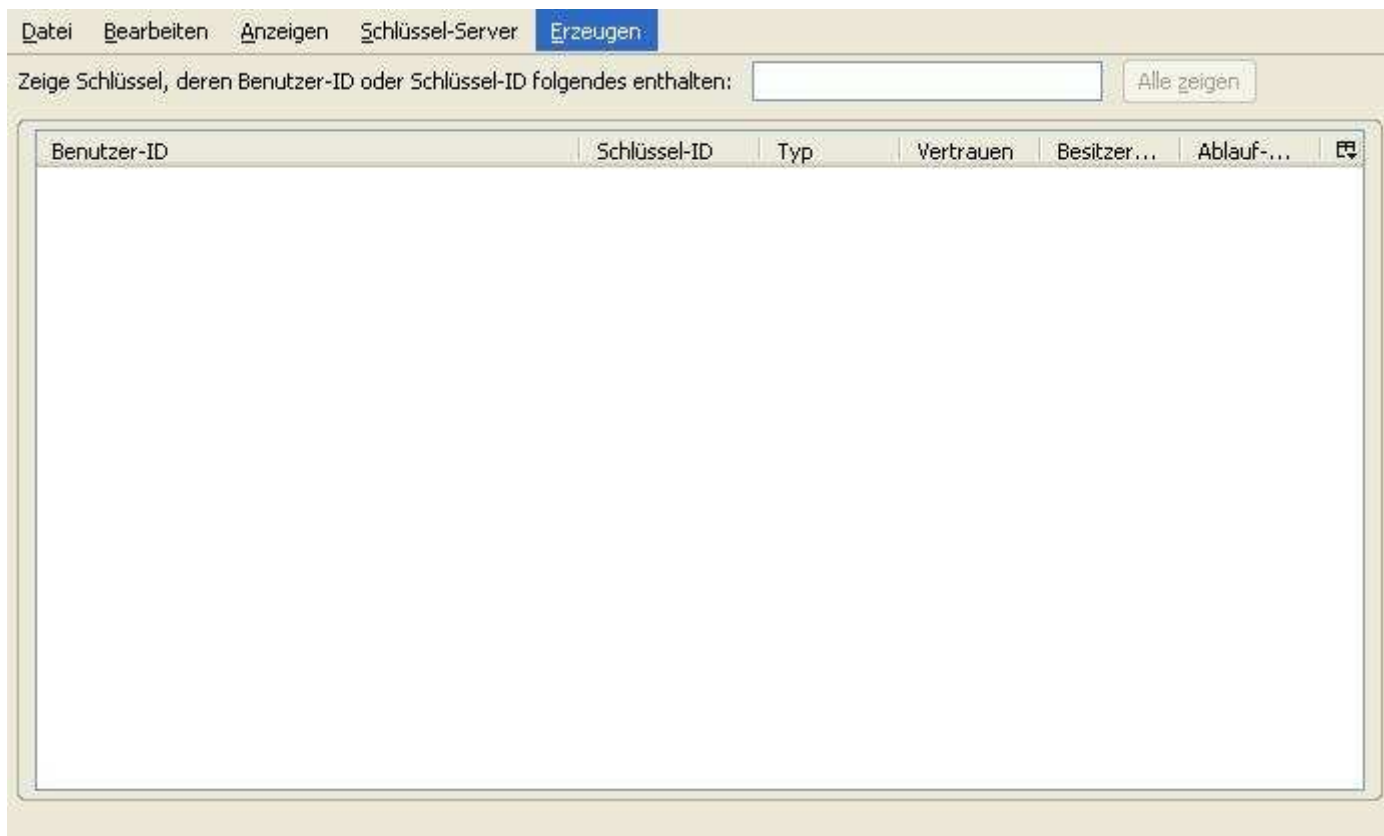
- 5.7. Nun Sie sehen untenstehenden Dialog. WICHTIG: Prüfen Sie, dass der Pfad heißt ".....\GnuPG\gpg.exe". Falls nicht, klicken Sie auf "Anderer Pfad" und stellen Sie den Pfad neu ein. Alles andere lassen, wie dargestellt.



- 5.8. Jetzt öffnen Sie die "Schlüssel verwalten" unter "OpenPGP".



5.9. Sie bekommen einen neuen Dialog:



5.10. Unter dem Menü-Punkt "Erzeugen" öffnen Sie "**Neues Schlüsselpaar**"



5.11. Wählen Sie den richtigen Benutzer-ID in dem Combo Box oben.

**OpenPGP-Schlüssel erzeugen**

Benutzer-ID: **KM <KM@eucars.de> - KM**

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase:  Passphrase wiederholen:

Kommentar:

Ablauf-Datum:  **Erweitert**

Schlüssel läuft ab in:     Schlüssel läuft nie ab

Konsole zum Erzeugen eines Schlüssels

**ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern.** Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.

- 5.12. Geben Sie einen Schlüssel ein. Es wird empfohlen mit "**KeePass**" ( Siehe separates Dokument "**GnuPG für NGOs in der Praxis**" ) einen Schlüssel zu generieren und danach diesen hinein zu kopieren.



Benutzer-ID KM <KM@eucars.de> - KM

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase \*\*\*\*\* Passphrase wiederholen \*\*\*\*\*

Kommentar

Ablauf-Datum

Schlüssel läuft ab in  Jahren  Schlüssel läuft nie ab

Konsole zum Erzeugen eines Schlüssels

**ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern.** Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.

- 5.13. Klicken Sie anschliessend auf "Schlüsselpaar erzeugen". Klicken Sie auf "Ja".



5.14. Warten Sie, bis das Schlüsselpaar erzeugt wird.

The screenshot shows a dialog box titled "OpenPGP-Schlüssel erzeugen". It contains the following fields and options:

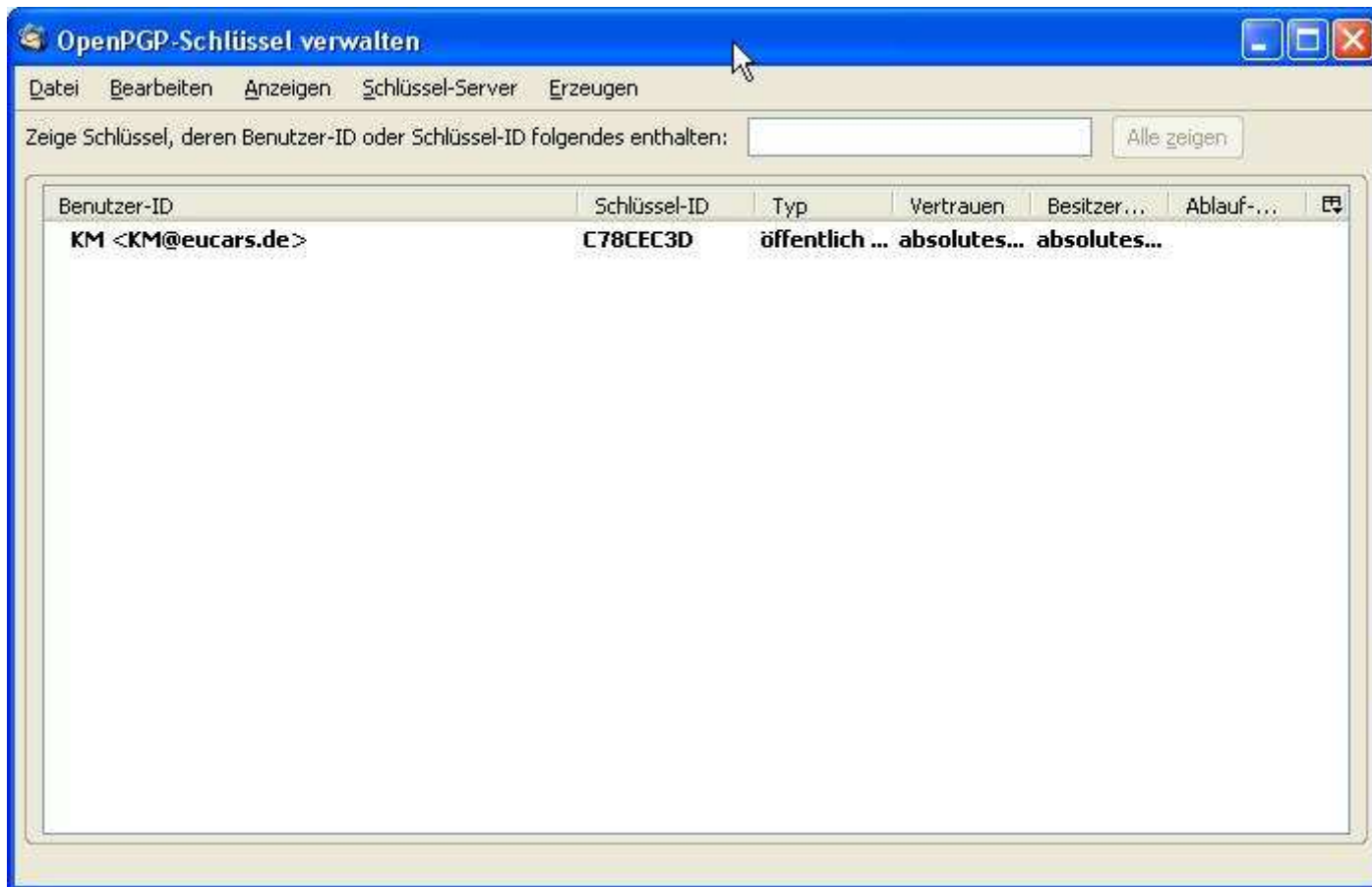
- Benutzer-ID: KM <KM@eucars.de> - KM
- Schlüssel zum Unterschreiben verwenden
- keine Passphrase
- Passphrase: \*\*\*\*\*
- Passphrase wiederholen: \*\*\*\*\*
- Kommentar: (empty text box)
- Ablauf-Datum:
- Schlüssel läuft ab in:  Jahren
- Schlüssel läuft nie ab
- Buttons: "Schlüsselpaar erzeugen" and "Abbrechen"
- Console area: "Kontrolle zum Erzeugen eines Schlüssels" with a warning: **ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern.** Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.
- A progress bar with 15 green segments.

5.15. Wenn der Rechner fertig ist, Klicken Sie "Ja" und speichern Sie das Widerrufs-zertifikat ab.

The screenshot shows a dialog box titled "OpenPGP-Bestätigung". It contains the following text and options:

- Icon: Question mark in a circle
- Text: Erzeugen des Schlüssels abgeschlossen. Benutzer-ID <KM@eucars.de> wird zum Unterschreiben verwendet.
- Text: Es wird dringend empfohlen, dass Sie nun ein Widerrufs-zertifikat für Ihren Schlüssel erzeugen. Dieses Zertifikat benötigen Sie, um Ihren Schlüssel bei Bedarf für ungültig zu erklären (z.B. wenn der Schlüssel missbraucht, verloren oder gestohlen wird).
- Text: Möchten Sie nun das zugehörige Widerrufs-zertifikat erzeugen?
- Buttons: "Ja" and "Nein"

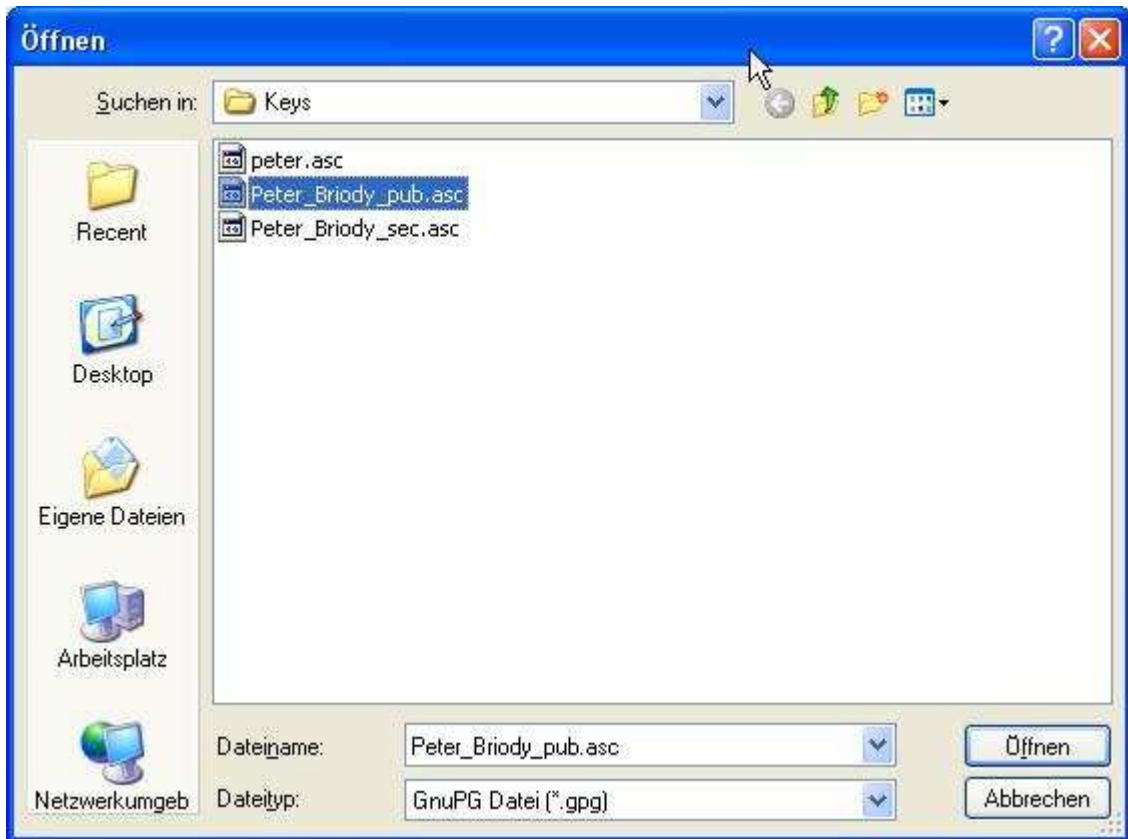
5.16. Nun sehen Sie den Dialog mit dem erfolgreich erzeugten Schlüsselpaar.



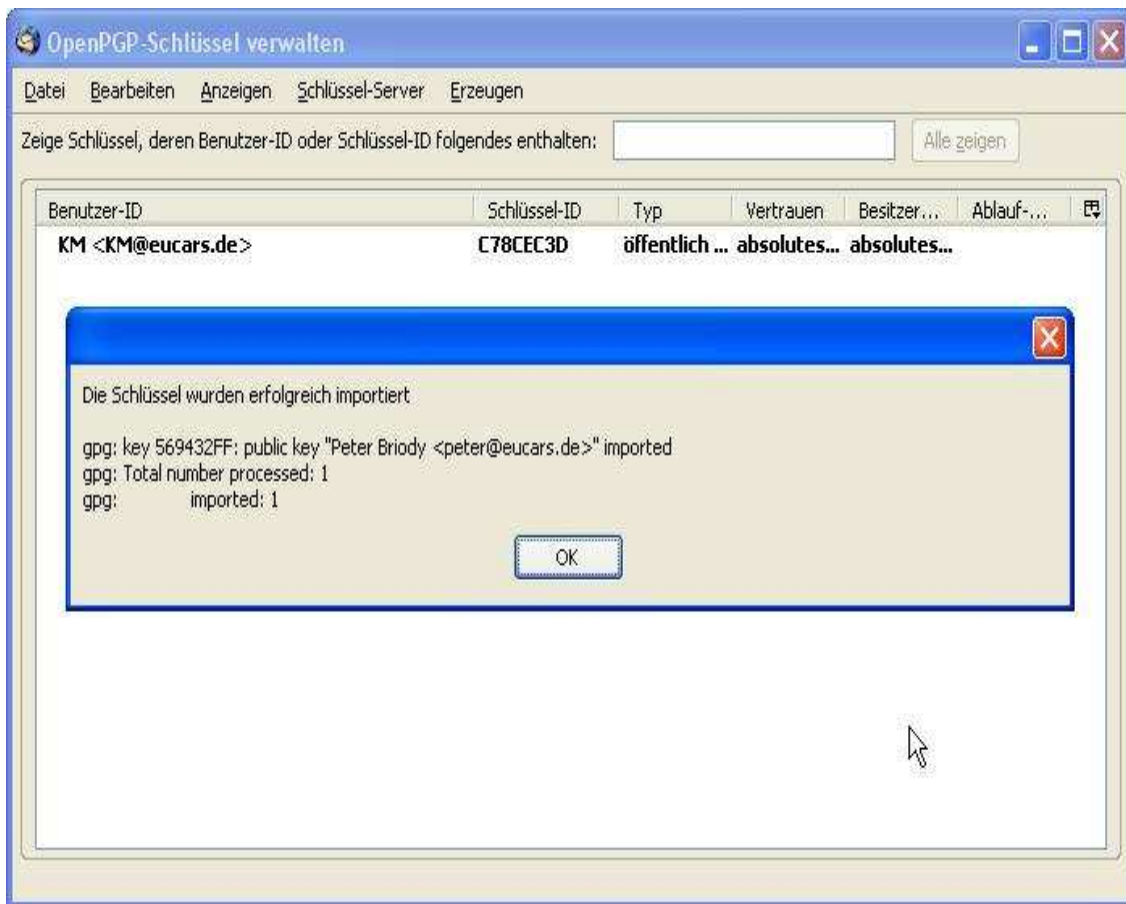
5.17. Klicken Sie auf "Importieren".



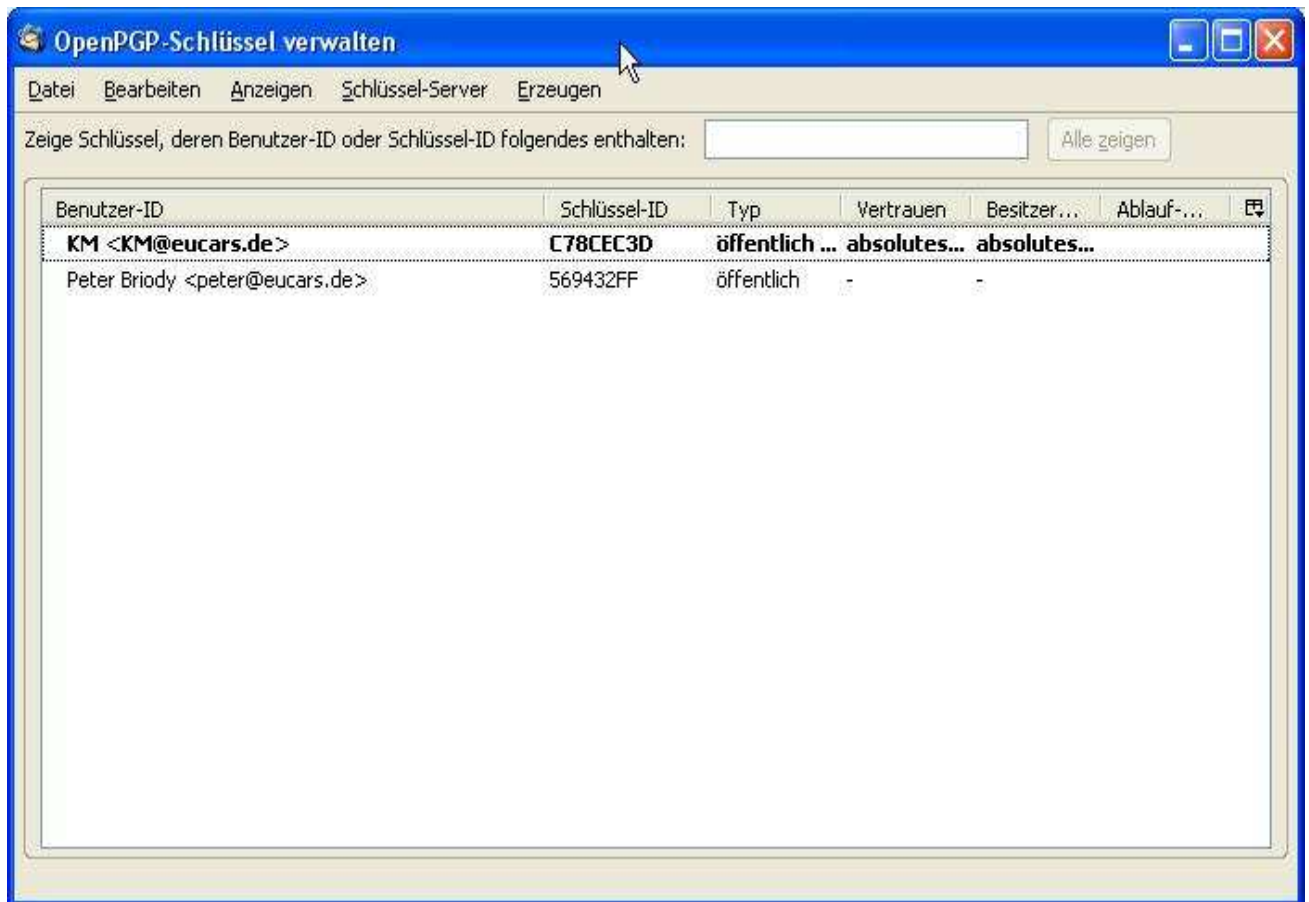
5.18. Suchen Sie einen "Öffentlichen Schlüssel", den man Ihnen per Vereinbarung geschickt hat.



5.19. Drücken Sie "Öffnen" und Sie sehen eine Zusammenfassung. Klicken Sie "OK".



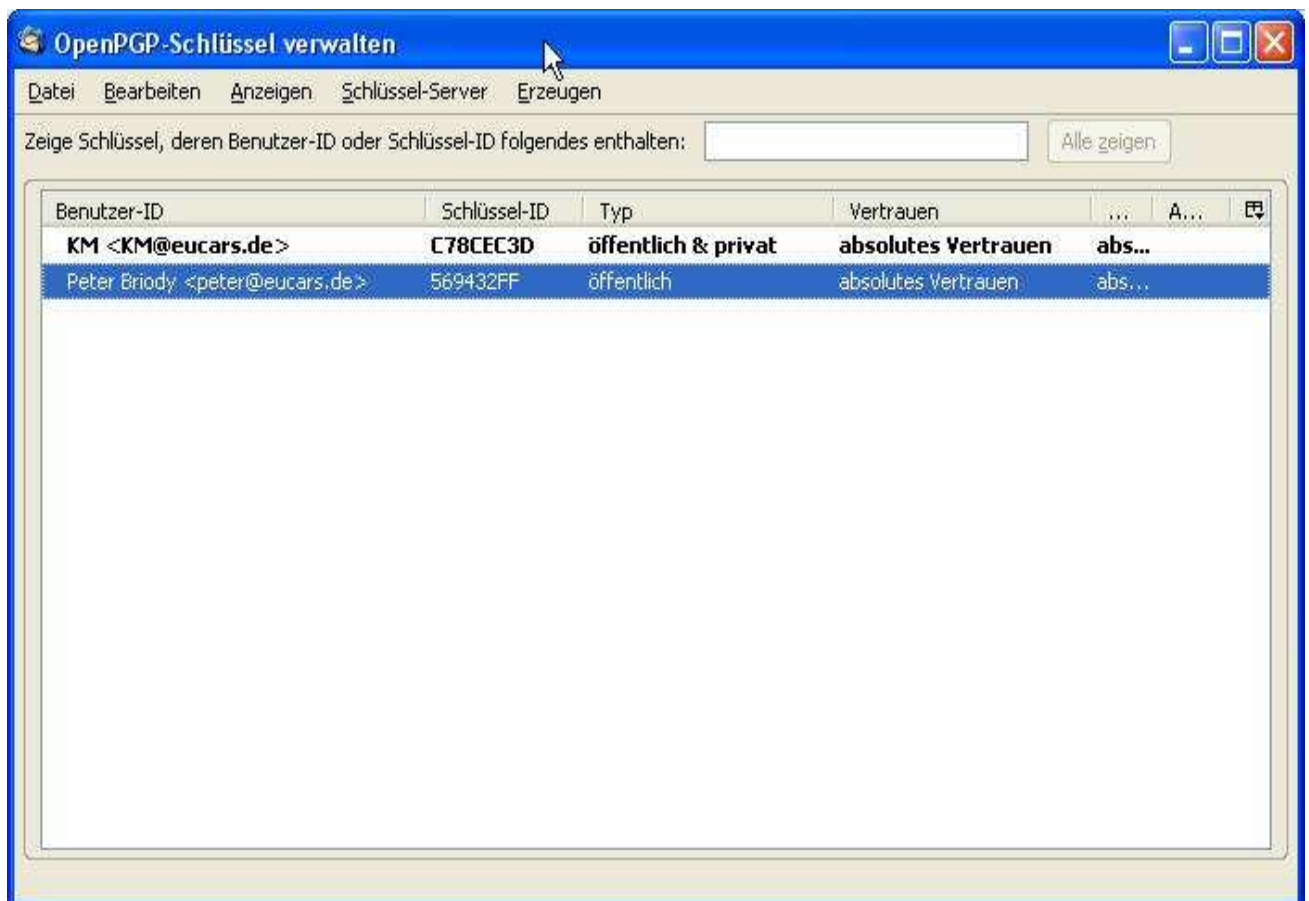
5.20. Jetzt sehen Sie Ihren Schlüssel und den Fremdschlüssel:



5.21. Jetzt können Sie den Fremdschlüssel "Unterschreiben" und, falls Sie dem Besitzer vertrauen, den "Besitzer-Vertrauen festlegen" drücken.



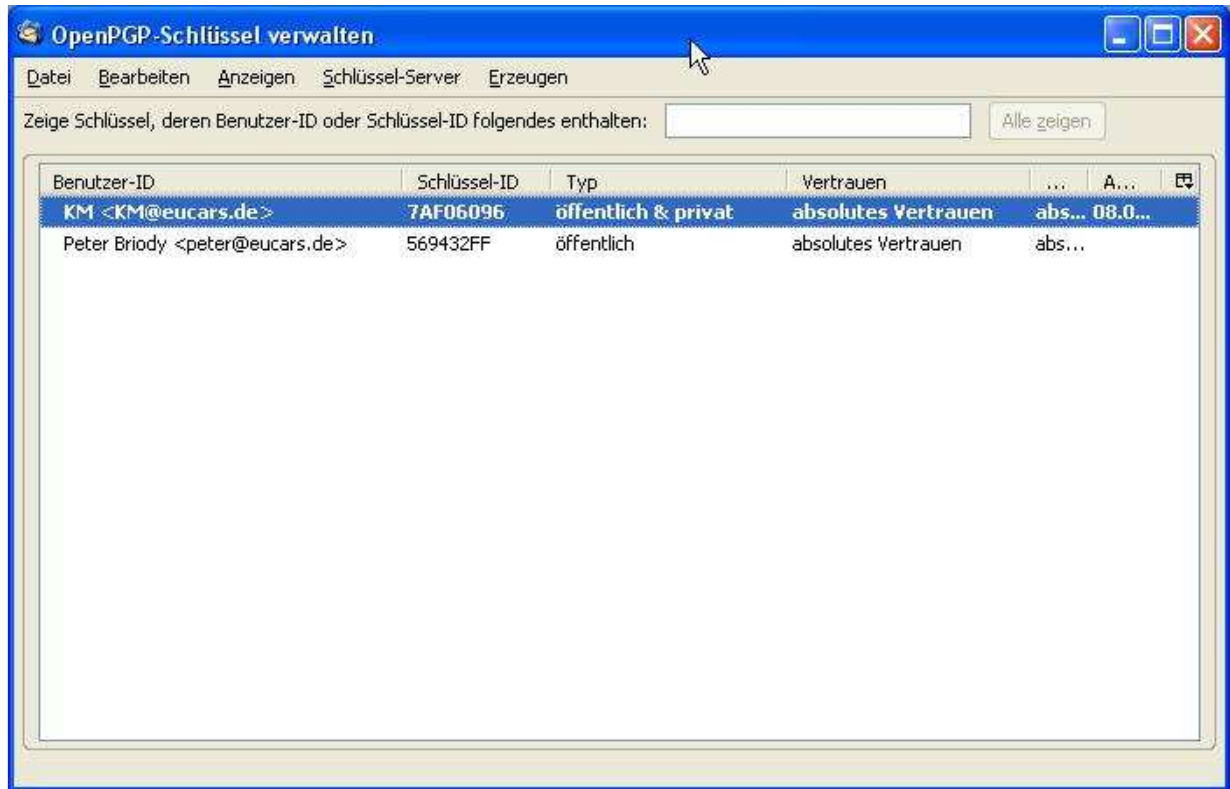
5.22. Sie sehen folgenden Dialog:



5.23. Glückwunsch, Sie haben es geschafft !

## 6. Anwendungsbeispiele

- 6.1. Angenommen Sie sind „KM“. Öffnen Sie die „**openPGP**“- Menü in Thunderbird. Wählen Sie „Schlüssel verwalten“ und Sie bekommen:



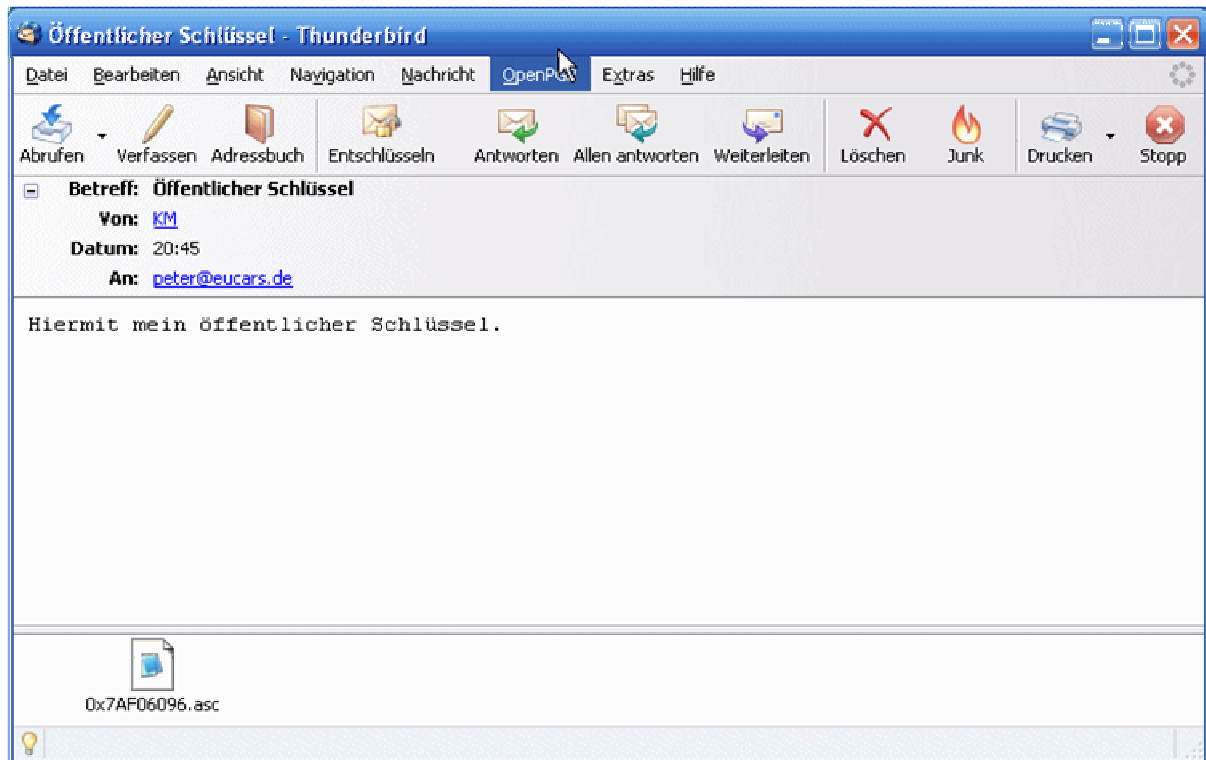
- 6.2. Klicken Sie auf „KM“ in den Dialog und wählen Sie in dem „**Datei**“-Menü „**Öffentliche Schlüssel per E-Mail senden**“.



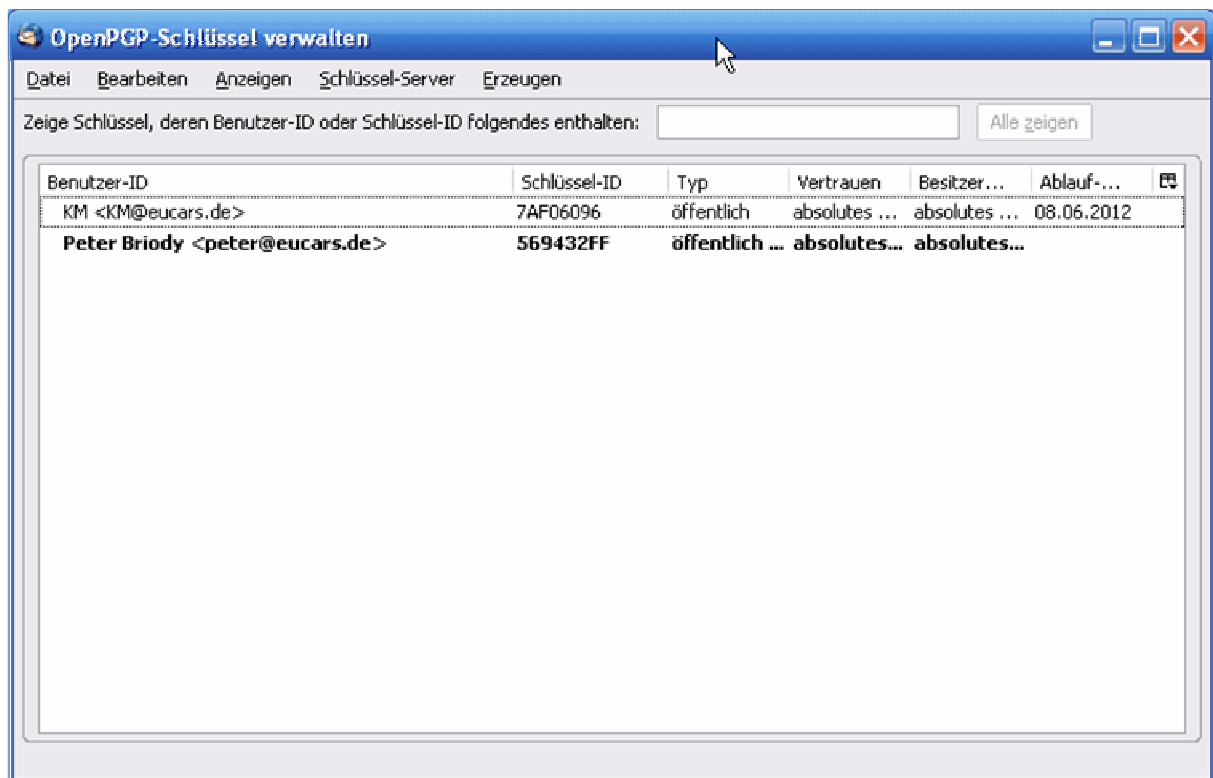
### 6.3. Sie senden die Mail:



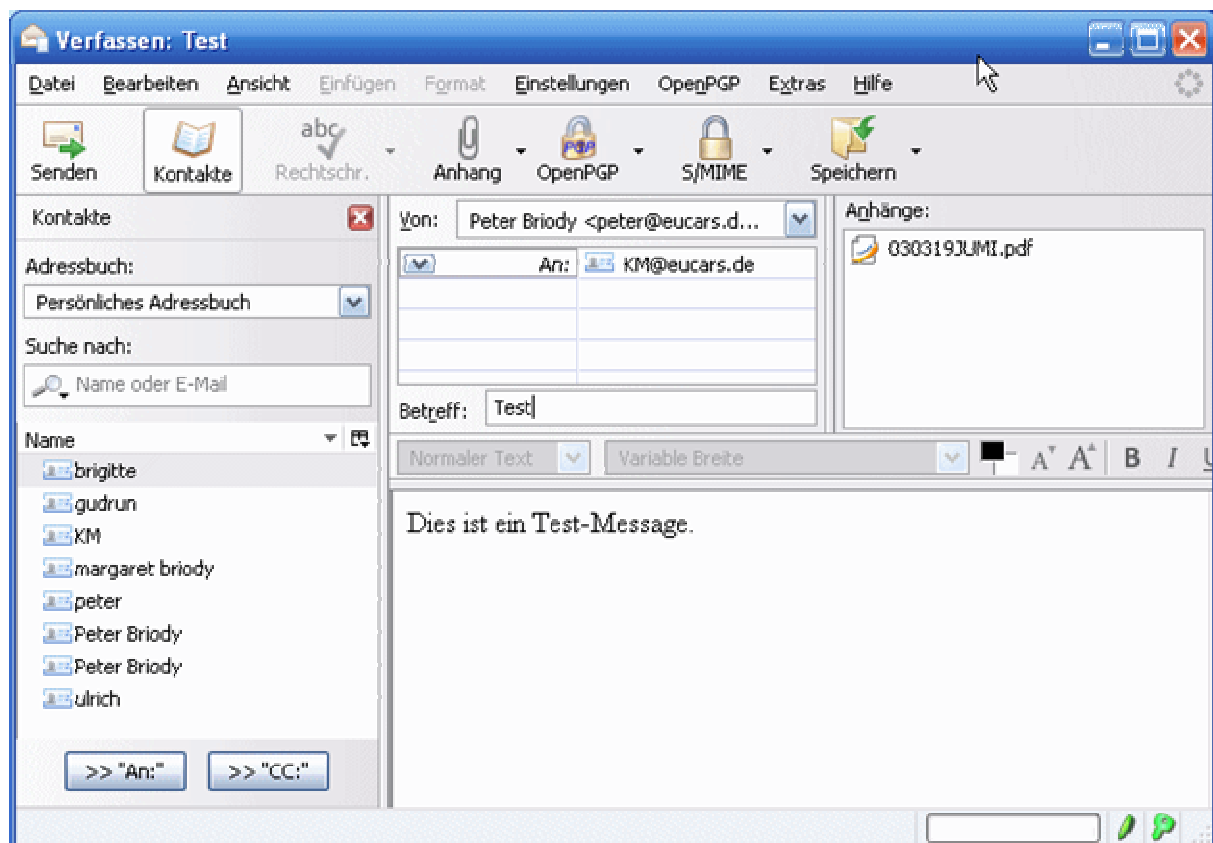
### 6.4. Angenommen, Sie sind „peter“ jetzt. Sie erhalten die Mail. Den Anhang speichern Sie irgendwo temporär ab und öffnen Sie „Schlüssel verwalten“ und importieren Sie den öffentlichen Schlüssel, die Sie von KM bekommen haben.



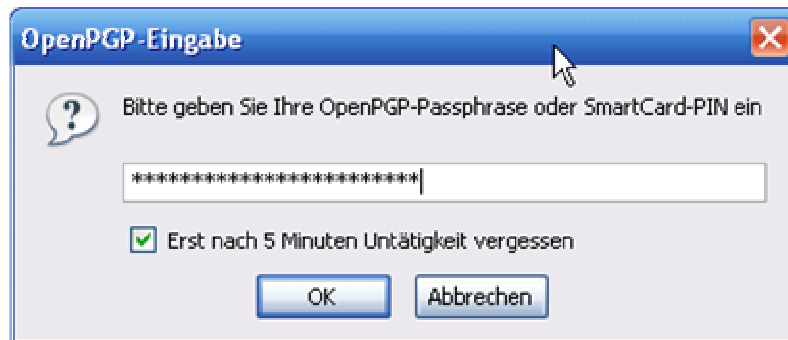
6.5. Sie sehen:



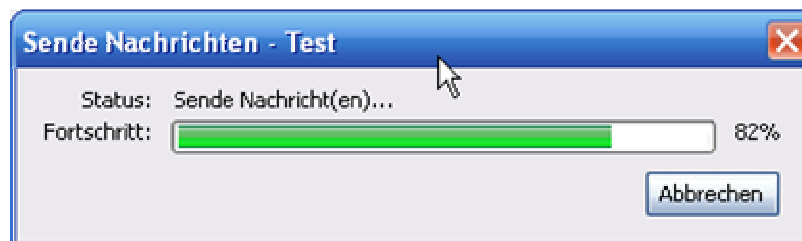
6.6. Nun sind Sie imstande, mit KM im Verschlüsselungsmodus zu kommunizieren - aber nur mit KM. Peter schickt eine E-Mail mit Anhang an KM Die Verschlüsselung wird mit den Grünen Zeichen unter rechts angezeigt.



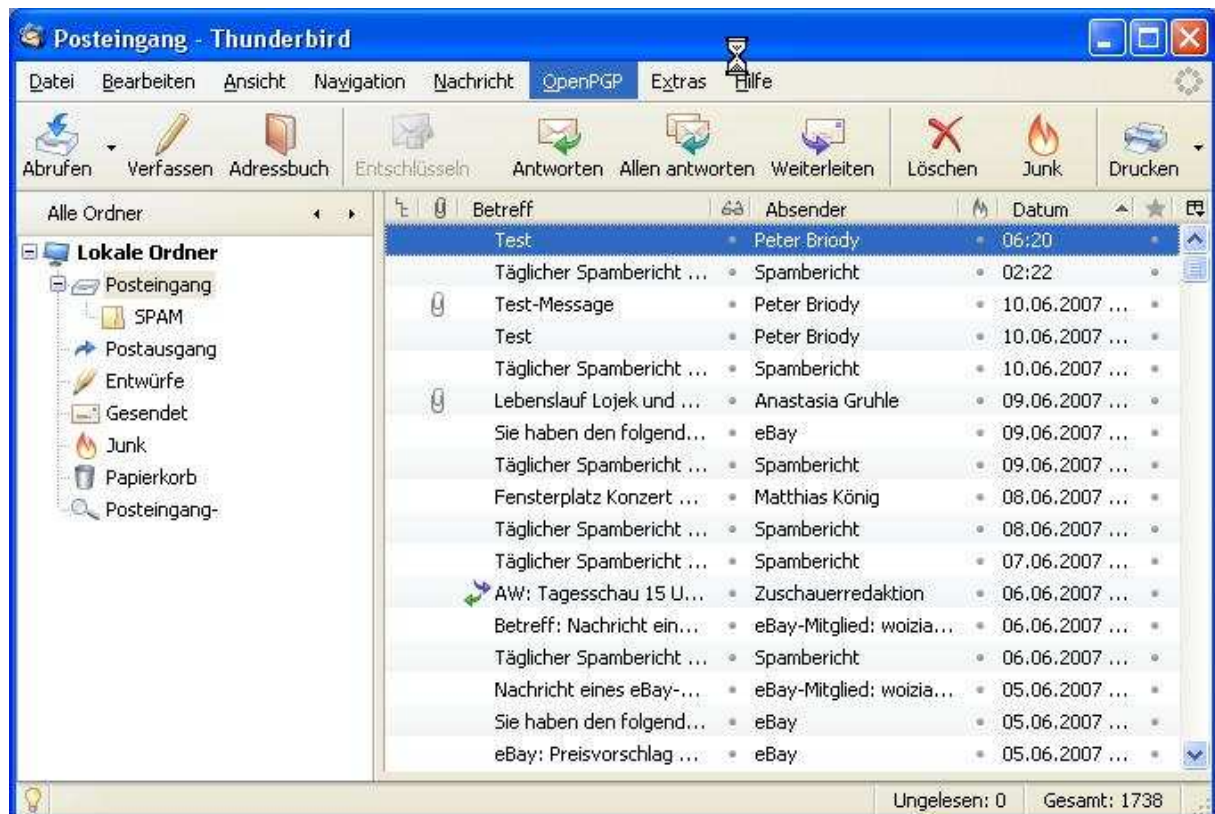
- 6.7. Falls Sie die Mail nicht verschlüsseln und / oder nicht unterschreiben möchten, dann klicken Sie je nachdem auf die grünen Icons. Sie ändern ihrer Farbe, dann zur Grau. Die Adresse, die Sie benutzen bestimmt automatisch den zu benutzenden Schlüssel. Der weitere Verlauf sieht folgendermaßen aus:



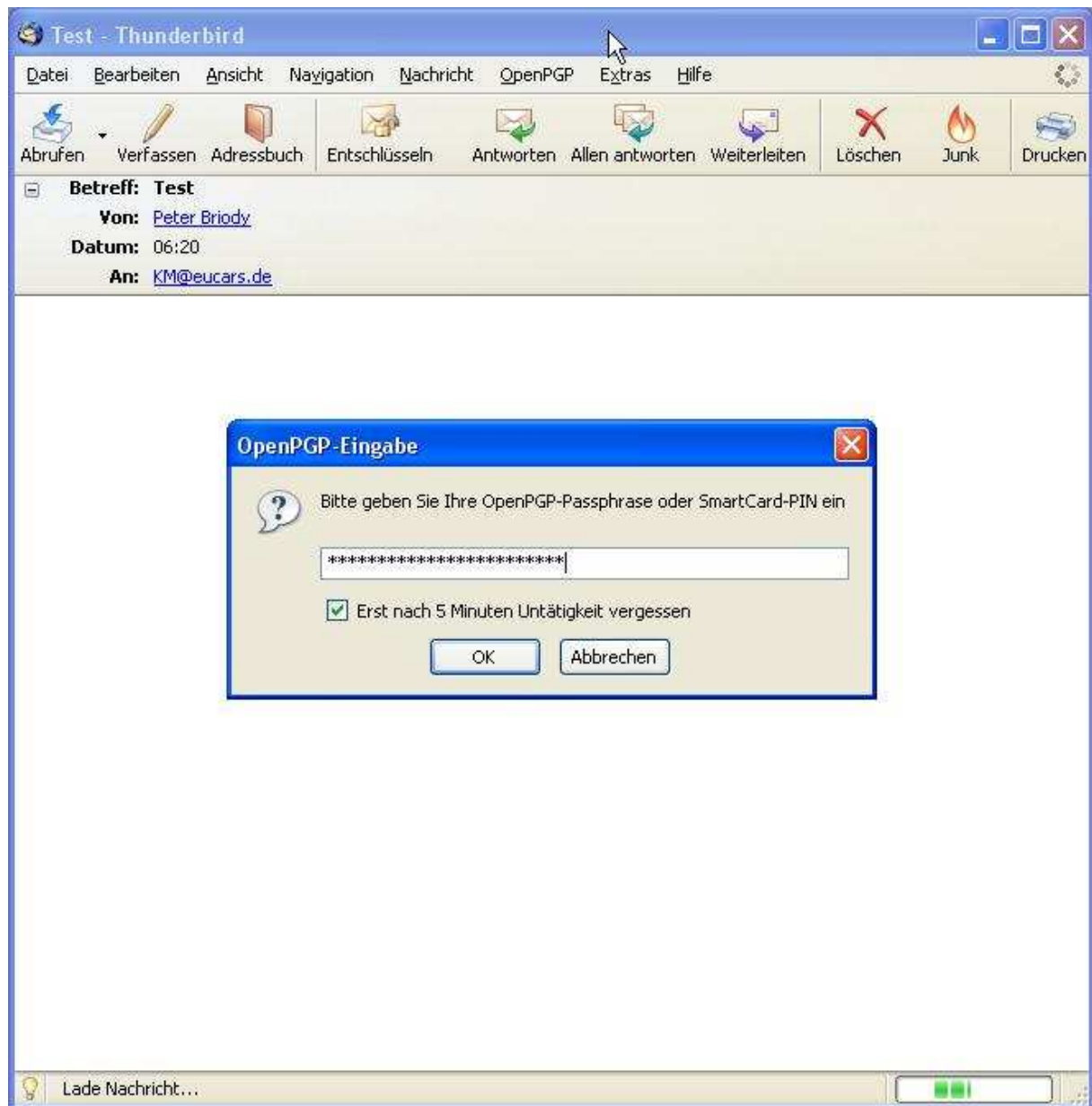
- 6.8. Kopieren Sie das Passwort aus KeePass oder was immer Sie für einen Panzerschrank Sie benutzen und klicken Sie „OK“. Sie sehen dann die Fortschrittsleiste und die verschlüsselte Mail wird an KM gesendet:



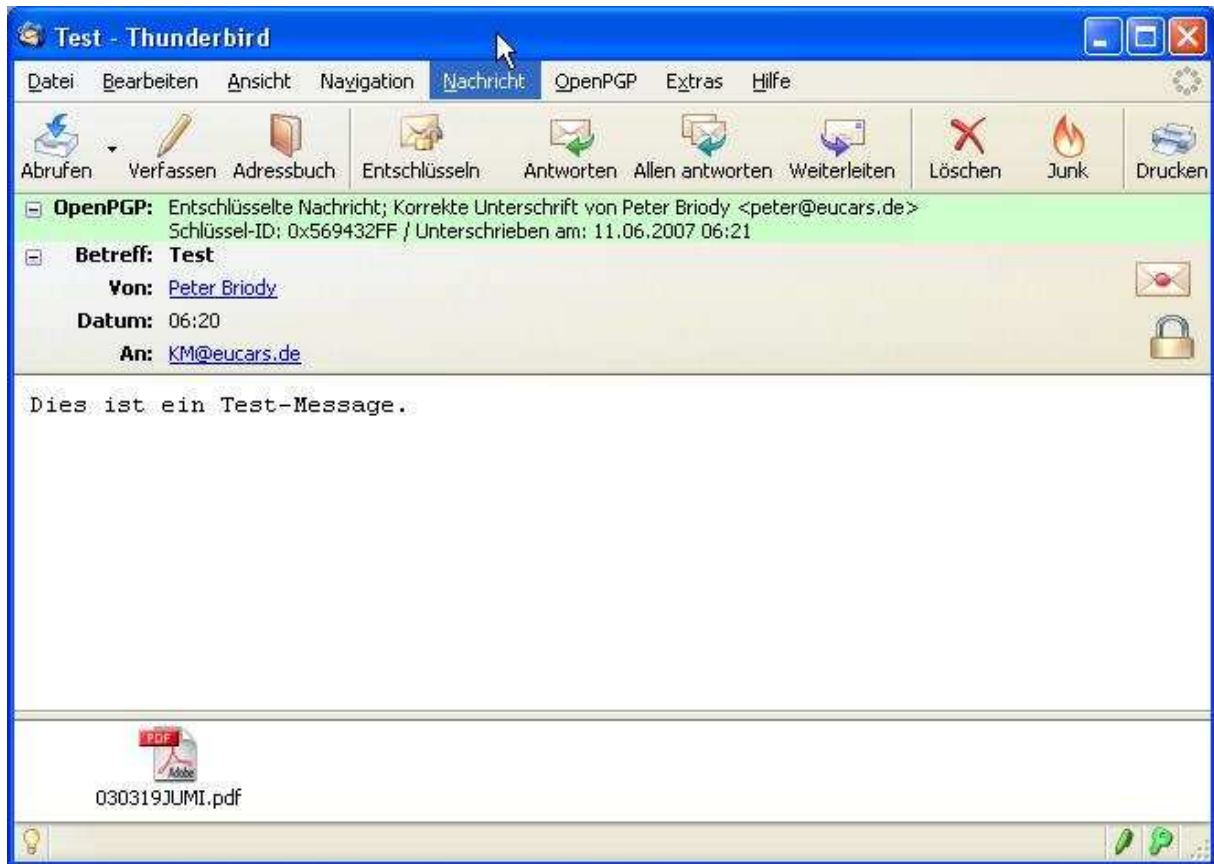
- 6.9. Auf dem Rechner von „KM“ kommt die Mail „Test“ an:



6.10. Nach Doppelklicken sieht es folgendermaßen aus. Sie geben die Passwort ein und drücken Sie auf „OK“:



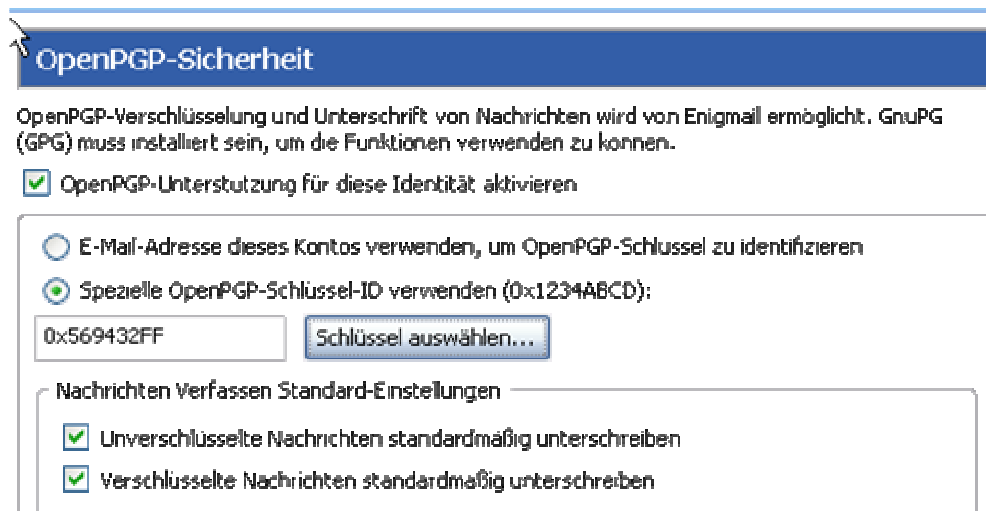
- 6.11. Sie sehen, dass das Bild jetzt ein bisschen anders aussieht, wie für Thunderbird normal ist. Ganz oben erhält man die Nachricht, dass es sich um eine verschlüsselte Mail handelt. Icons erscheinen auf der Adresseleiste und unten rechts auf der Statusleiste. Die Mail wurde automatisch entschlüsselt.



- 6.12. Falls man von KMs Rechner an Peter eine Mail schicke würde, passierte das Gleiche – nur dass andere Schlüssel verwendet werde würden. Man kann so viele Ansprechpartner einstellen, wie man will.

## 7. Synchronisierung

- 7.1. Synchronisierung ist oftmals notwendig, z.B. zwecks Abstimmung von Unterlagen sowie für größere Projekte, wo die Sendung von mehrfachen Mails separat an Individuen einen zu großen Aufwand bedeuten würde. Diese Aktion bedarf allerdings genaue Behandlung durch eine(n) Projektleiter(in).
- 7.2. Jedem Projektteilnehmer muss der private Schlüssel des Projektleiters sowie das Passwort bekommen. Dies kann nur im Verschlüsselten Modus nach dem üblichen Austausch der öffentlichen Schlüssel mit jedem Projektbeteiligten stattfinden. Darüber hinaus muss man die Kontoeinstellungen ändern, weil die Zuordnung der Schlüssel nach E-Mail-Adresse nicht mehr gültig ist: Man muss stattdessen die ID des Schlüssels verwenden ( Siehe unten ).



**OpenPGP-Sicherheit**

OpenPGP-Verschlüsselung und Unterschrift von Nachrichten wird von Enigmail ermöglicht. GnuPG (GPG) muss installiert sein, um die Funktionen verwenden zu können.

OpenPGP-Unterstützung für diese Identität aktivieren

E-Mail-Adresse dieses Kontos verwenden, um OpenPGP-Schlüssel zu identifizieren

Spezielle OpenPGP-Schlüssel-ID verwenden (0x1234ABCD):

Nachrichten Verfassen Standard-Einstellungen

Unverschlüsselte Nachrichten standardmäßig unterschreiben

Verschlüsselte Nachrichten standardmäßig unterschreiben