

# Verschlüsselte Email-Kommunikation mit Mozilla/Enigmail und GnuPG

Jan Dittberner <jan@dittberner.info>

25. Juni 2003

Dieses Dokument beschreibt die Einrichtung und Anwendung des Mozilla-Mail-Clients, mit dem Verschlüsselungswerkzeug GnuPG und dem Enigmail Plugin unter Microsoft® Windows®.

## Inhaltsverzeichnis

<b>1</b>	<b>Softwareversionen</b>	<b>1</b>
<b>2</b>	<b>Installation</b>	<b>2</b>
2.1	GnuPG installieren . . . . .	2
2.2	Mozilla installieren . . . . .	2
2.3	Enigmail und Enigmime installieren . . . . .	5
<b>3</b>	<b>Schlüssel generieren und exportieren</b>	<b>6</b>
3.1	Schlüssel mit GnuPG generieren . . . . .	6
3.2	Schlüssel an Keyserver senden . . . . .	7
<b>4</b>	<b>Enigmail für die Benutzung mit GnuPG einrichten</b>	<b>8</b>
<b>5</b>	<b>Mail schreiben, signieren, verschlüsseln</b>	<b>9</b>

## 1 Softwareversionen

Folgende Softwareversionen wurden für die Erstellung dieses Dokumentes genutzt

- GnuPG 1.2.1
- Mozilla 1.3 (de-AT)
- Enigmail 0.74.0
- Enigmime 0.74.0

## 2 Installation

Zur Installation sollten sie so vorgehen:

### 2.1 GnuPG installieren

1. Laden Sie sich das Installationsfile von <http://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.2.1-1.zip> herunter.
2. Unter Windows XP können Sie dieses File einfach mit dem Windows-Explorer öffnen. Unter älteren Windows-Versionen benötigen Sie dafür ein Zip-Programm (z.B. WinZip).
3. Entpacken Sie die Dateien aus dem Zip-Archiv in ein Verzeichnis auf Ihrer Festplatte. In dieser Anleitung wird `C:\GnuPG` verwendet.
4. Doppelklicken Sie im Windows-Explorer auf die Datei `gnupg-w32.reg` und klicken Sie auf *Ja* um die Schlüssel in Ihrer Windows Registry einzutragen. Sollten Sie GnuPG in einem anderen Verzeichnis als `C:\GnuPG` installiert haben, müssen Sie die Pfade in der `gnupg-w32.reg`-Datei ändern

### 2.2 Mozilla installieren

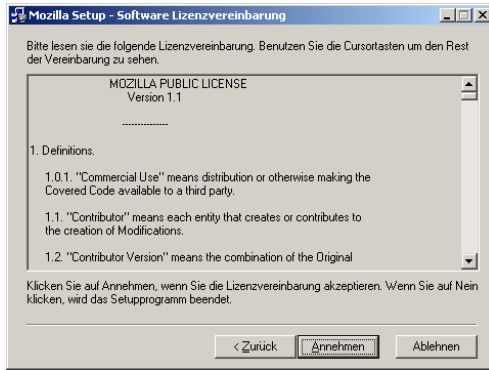
<http://ftp.mozilla.org/pub/mozilla/110n/lang/moz1.3/mozilla-win32-1.3-deAT-installer.exe> heruntergeladene Installationsprogramm und gehen Sie folgendermaßen vor:

1. Sie sehen den Startbildschirm,



klicken Sie auf *Weiter*.

2. Sie sehen die Lizenzbedingungen,



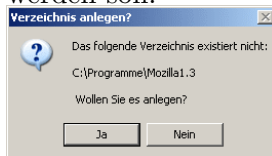
lesen Sie diese und klicken Sie auf *Annehmen*.

3. Sie haben die Auswahl welche Teile von Mozilla Sie installieren möchten.



Wählen Sie *Normal* oder *Benutzerdefiniert* und klicken Sie auf *Weiter*.

4. Sie werden jetzt gefragt, ob das Verzeichnis für die Installation angelegt werden soll.



Klicken Sie auf *Ja*

5. Sollten Sie im vorletzten Schritt *Benutzerdefiniert* gewählt haben, können Sie jetzt auswählen welche Teile Sie installieren möchten.



Für unsere Zwecke wird der *Mail & Newsgroups*-Teil benötigt. Der *Navigator* wird immer mitinstalliert. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf *Weiter*.

6. Jetzt können Sie wählen, in welchem Teil des Windowsstartmenüs Mozilla eingetragen wird.



Belassen Sie die Auswahl bei *Mozilla* oder ändern Sie diesen Eintrag auf einen anderen von Ihnen gewünschten Wert und klicken Sie auf *Weiter*.

7. Jetzt werden Sie gefragt, ob der Mozilla-Schnellstart aktiviert werden soll.



Klicken Sie auf *Weiter*.

8. Eine Zusammenfassung der von Ihnen getroffenen Einstellungen wird angezeigt,



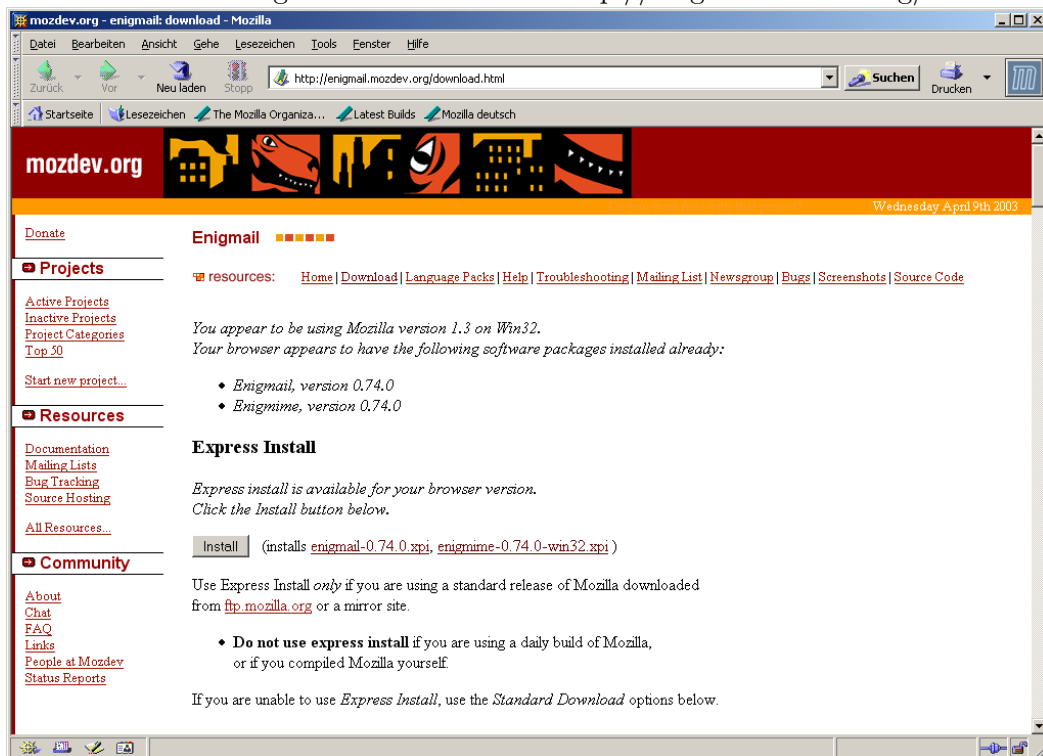
klicken Sie auf *Installieren*.

9. Nun wird die Installation durchgeführt.

## 2.3 Enigmail und Enigmime installieren

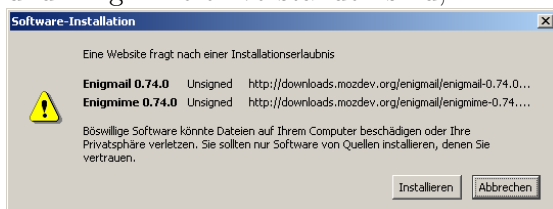
Enigmail und Enigmime sind die Bestandteile des Mozilla Plugins, die benötigt werden um mit GnuPG verschlüsselte oder signierte Emails aus dem Mozilla-Mailer zu versenden.

1. zum Beginn der Installation von Enigmail und Enigmime starten Sie den Mozilla-Browser und gehen Sie auf den URL <http://enigmail.mozdev.org/download.html>



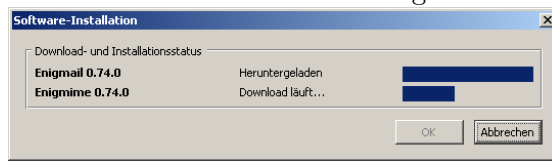
Ihr Browser sollte automatisch erkannt werden und Sie sollten obige Seite zu sehen bekommen. Klicken Sie unter *Express Install* auf den grauen *Install*-Knopf.

2. Daraufhin werden Sie gefragt, ob Sie mit der Installation von Enigmail und Enigmime einverstanden sind,

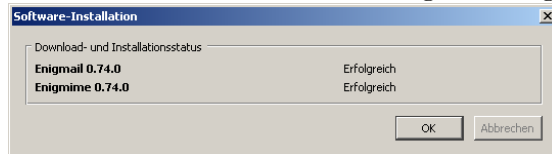


klicken Sie auf *Installieren*

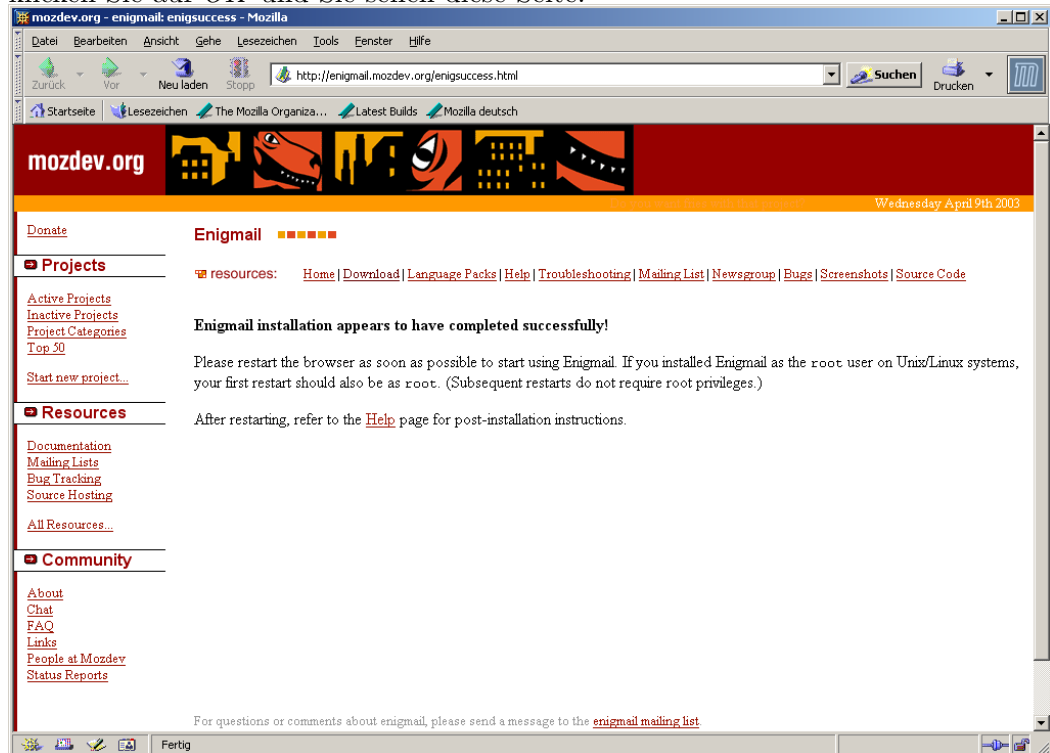
3. Die Installation wird nun durchgeführt.



4. Zum Abschluss sollte diese Erfolgsmeldung zu sehen sein:



klicken Sie auf *OK* und Sie sehen diese Seite:



damit ist die Installation abgeschlossen. Schließen Sie den Mozilla-Browser jetzt, damit Enigmail beim nächsten Start von Mozilla mit geladen werden kann.

## 3 Schlüssel generieren und exportieren

### 3.1 Schlüssel mit GnuPG generieren

Öffnen Sie ein Kommandozeilenfenster **Startmenü - Ausführen...** unter Windows NT/2000/XP mit `cmd` und unter Windows 95/98/ME `command`  
Wechseln Sie in das GnuPG Verzeichnis

```
cd C:\GnuPG
```

Geben Sie ein

```
gpg -gen-key
```

Akzeptieren Sie per Enter-Taste die Standardeinstellungen für Schlüsseltyp (DSA und Elgamal), Schlüssellänge (1024 bit) und Gültigkeit (unbegrenzt). Bestätigen Sie diese Angaben mit *j*

Geben Sie nun Ihren Vor- und Nachname ein. Es ist wichtig, dass Sie hier Ihren richtigen Namen eintragen, da dies wesentlich zum Vertrauen anderer PGP/GnuPG-Nutzer beiträgt.

Jetzt geben Sie bitte Ihre Email-Adresse an. Verwenden Sie, wenn Sie über mehrere Email-Adressen verfügen, für diesen Zweck die von Ihnen am häufigsten genutzte Adresse. Es ist möglich dem Schlüssel später weitere Emailadressen als sogenannte *subkeys* zuzuordnen. Damit können Sie einen Schlüssel auch für verschiedene Adressen verwenden.

Nun werden Sie nach einem Kommentar für den Schlüssel gefragt. Diesen können Sie auch leerlassen, oder ihm einen nützlichen Text wie z.B. "Adresse in der Firma" zuweisen.

Sie werden nun noch einmal gefragt, ob die von Ihnen gemachten Angaben in Ordnung sind. Wenn Sie sich von der Korrektheit der Daten überzeugt haben bestätigen Sie mit *F*.

Nun werden Sie nach dem Mantra gefragt. Das ist ein Passwortsatz. Dieser wird von Ihnen für folgende Aktionen benötigt:

- Signieren von Mails, Dateien oder Public-Keys anderer PGP/GnuPG-Nutzer
- Lesen von verschlüsselten Emails an Ihre Adresse(n)
- Ändern Ihres Schlüssels

. Wie Sie sehen hat das Mantra entscheidenden Einfluss auf die Sicherheit Ihres Schlüssels. Das Mantra sollten Sie sich gut merken können, es sollte jedoch nicht zu kurz sein (um Angriffe durch Brute-Force ("Rohe Gewalt"), also probieren auszuschließen) und es sollte auch nicht durch Personen aus Ihrem Umfeld leicht zu erraten sein.

Sie müssen das Mantra noch ein zweites Mal eingeben, um Fehleingaben zu vermeiden. Danach wird der Schlüssel erzeugt.

Zum Schluss werden die Schlüssel-Ids der privaten und öffentlichen Schlüssel angezeigt, damit ist die Schlüsselerzeugung abgeschlossen.

### 3.2 Schlüssel an Keyserver senden

Um Ihren öffentlichen Schlüssel (public key) an einen der pgp.net Keyserver zu schicken geben Sie folgenden Befehl auf der Kommandozeile ein

```
gpg -keyserver hkp://wwwkeys.de.pgp.net --send-keys <num>
```

anstelle von *<num>* müssen Sie hier die Nummer ihres öffentlichen Schlüssels angeben. Diese Nummer finden Sie, wenn Sie

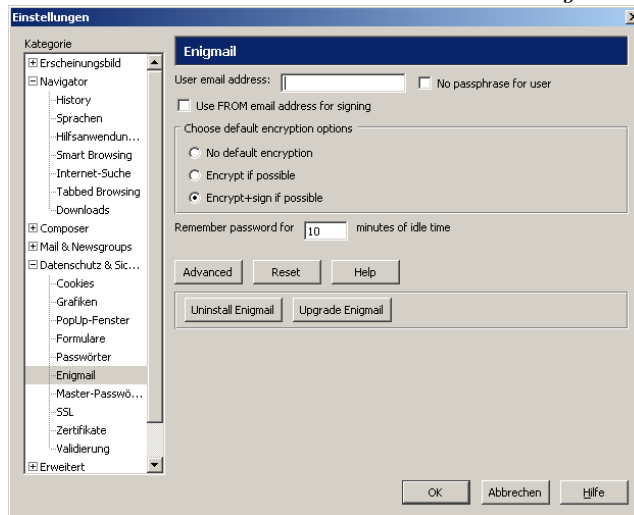
`gpg -list-keys <email@adres.se>`  
ausführen. Die Keyid steht hinter dem Wort `pub` z.B.

```
C:\GnuPG>gpg --list-keys klaus.testperson@test.example
pub 1024D/4F1B9117 2003-04-09 Klaus Testperson (Adresse in der Firma) <klaus.te
sub 1024g/037BC469 2003-04-09
```

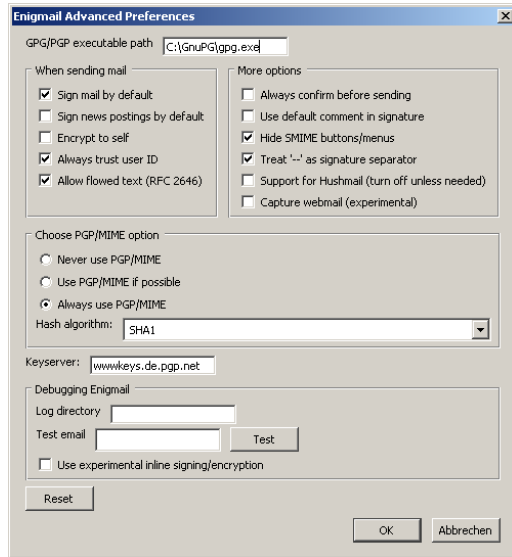
hier wäre die Keyid 4F1B9117 also  
`gpg -keyserver hkp://wwwkeys.de.pgp.net -send-keys 4F1B9117`

## 4 Enigmail für die Benutzung mit GnuPG einrichten

- Starten Sie Mozilla.
- Öffnen Sie im Menü *Bearbeiten* den Punkt *Einstellungen...*
- Wählen Sie *Datenschutz & Sicherheit - Enigmail*



- Geben Sie bei "User email address:" die Adresse an, die Sie für Ihren GnuPG-Schlüssel verwendet haben.
- Wählen Sie aus, ob Sie Emails standardmäßig nicht verschlüsseln, nur verschlüsseln oder verschlüsseln und signieren wollen.
- Klicken Sie auf *Advanced*. Es öffnet sich dieser Bildschirm:



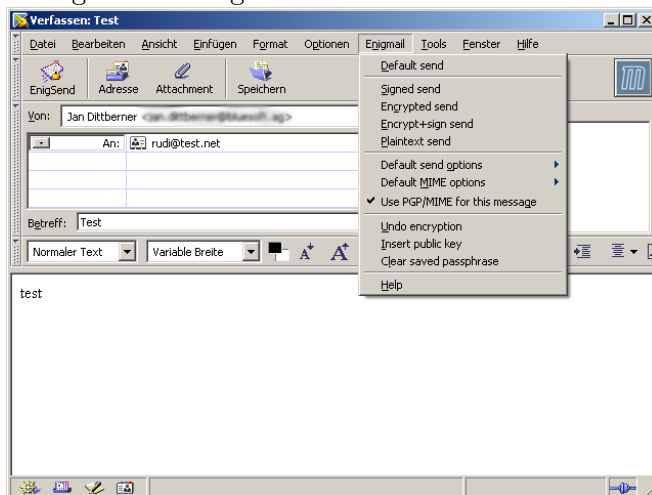
Tragen Sie unter “GPG/PGP executable path” C:\GnuPG\gpg.exe ein. Alle anderen Einstellungen können Sie bei den Voreinstellungen belassen.

- Klicken Sie auf *OK*, um die Einstellungen zu übernehmen und noch einmal auf *OK*, um den Einstellungen Dialog zu schließen.

## 5 Mail schreiben, signieren, verschlüsseln

Eine Email können Sie in Mozilla schreiben, indem Sie über das Menü *Datei - Neu - Nachricht* ein neues Email-Fenster öffnen. Schreiben Sie ganz normal Empfänger, Betreff und Inhalt ihrer Mail, hängen Sie gegebenenfalls noch Anhänge an die Mail an.

Im Menü Enigmail gibt es eine Reihe von Möglichkeiten für die Verschlüsselung und das Signieren Ihrer Nachricht.



- Default Send** Ist das gleiche wie wenn Sie auf den *EnigSend*-Knopf klicken, also die Einstellung aus dem “Enigmail”-Einstellungsdialog
- Signed Send** Verschickt die Mail unverschlüsselt, aber mit Ihrem Schlüssel unterschrieben, damit kann ein Empfänger prüfen, ob die Mail wirklich von Ihnen stammt, wenn er Ihren Public-Key hat (z.B. von einem Keyserver 3.2 oder aus einer Mail von Ihnen). Sie werden nach Ihrem Mantra gefragt.
- Encrypted Send** Sendet eine verschlüsselte Email.
- Encrypted+Sign Send** Sendet eine verschlüsselte und signierte Email.
- Plaintext Send** Sendet eine Email im Klartext.
- Use PGP/MIME for this message** Es gibt zwei Verfahren für PGP/GPG Signaturen, die Signatur kann entweder in den Mailtext eingebettet werden oder als Anhang (MIME-Mail) zur Mail hinzugefügt werden. Einige Mailprogramme haben Probleme mit PGP/MIME, deshalb ist es ab und an ratsam diese Option auszuschalten.
- Undo encryption** Entschlüsselt eine verschlüsselte Mail wieder.
- Insert public key** Fügt Ihren öffentlichen Schlüssel zu der Mail hinzu. Wenn Sie jemandem zum ersten Mal eine Email mit Ihrem Schlüssel schicken, ist das eine gute Möglichkeit ihm den Schlüssel zu übergeben. Die Variante mit den Keyservern von oben ist aber flexibler.
- Clear saved passphrase** Wenn Sie das Mantra für Ihren Schlüssel eingegeben haben, merkt sich Enigmail diesen für einige Zeit. Mit dieser Option können Sie Enigmail das Mantra vergessen lassen.