

Anleitung Thunderbird Email Verschlüsselung

Christoph Weinandt, Darmstadt

Vorbemerkung

Diese Anleitung beschreibt die Einrichtung des AddOn's „Enigmail“ für den Mailclient Thunderbird. Diese Anleitung gilt unabhängig vom verwendeten Betriebssystem und setzt die Installation des GnuPG Programmes voraus, welches die technische Infrastruktur zur Verschlüsselung bereitstellt. In dieser Anleitung ist die Einrichtung des Addon's „Enigmail“, die Erstellung des eigenen Schlüsselpaares und die beispielhafte Ver- und Entschlüsselung von Emails beschrieben.

Softwarequellen

Für Thunderbird: <https://www.mozilla.org/de/thunderbird/>

Für Enigmail: bitte via Thunderbird -> AddOn's runterladen und installieren



The image shows a promotional banner for Thunderbird on the left and a Windows file dialog on the right. The banner features the text "Software für den einfachen Umgang mit E-Mails." and "Thunderbird ist eine freie E-Mail-Anwendung, die man einfach einrichten und anpassen kann — und sie ist voll mit tollen Funktionen!". Below this is the Thunderbird logo and a green button that says "Thunderbird Kostenloser Download". At the bottom of the banner, it says "Versionshinweise · Andere Systeme & Sprachen". The dialog box is titled "Öffnen von Thunderbird Setup 24.1.0.exe" and asks "Sie möchten folgende Datei öffnen:". It lists the file "Thunderbird Setup 24.1.0.exe" as a "Binary File (21,0 MB)" from "http://download-installer.cdn.mozilla.net". It asks "Möchten Sie diese Datei speichern?" and has "Datei speichern" and "Abbrechen" buttons. At the bottom of the dialog, it says "Datenschutzrichtlinie | Rechtliche Hinweise" and "Copyright © 2005–2013 Mozilla. Alle Rechte vorbehalten."

Installation

Die Installation von Thunderbird erfolgt mit den vorgewählten Einstellungen. Anschliessend ist im Menü „Add-ons“ das „Enigmail“ auszuwählen und zu installieren:



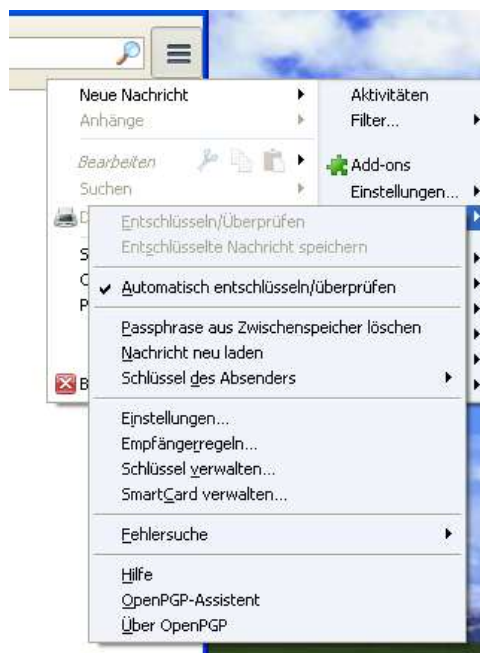
Nachdem Thunderbird neu gestartet wurde, ist ein Emailkonto einzurichten – dazu sehen Sie bitte in dem WIKI des Thunderbird Programmes nach:

<http://www.thunderbird-mail.de/wiki/Dokumentation>

oder folgen Sie dieser Anleitung – je nachdem, ob Sie POP oder IMAP benutzen:

http://www.thunderbird-mail.de/wiki/E-Mail-POP-Konto_einrichten_ab_Thunderbird_3.0

http://www.thunderbird-mail.de/wiki/E-Mail-IMAP-Konto_einrichten_ab_Thunderbird_3.0



Sie können für jedes konfigurierte Konto separat die Verschlüsselung konfigurieren. Dazu gehen Sie auf die Einstellungen:

Hier können Sie das Addon konfigurieren und können Ihre Schlüssel verwalten, neue öffentliche Schlüssel herunterladen und sämtliche Aspekte der Emailverschlüsselung überwachen. Es gibt zwei „default“ Einstellungen, die wichtig sind und unverändert gelassen werden sollten: neben dem Häkchen bei „automatisch entschlüsseln/überprüfen“ ist dies die Einstellung „mit dem eigenen Schlüssel verschlüsseln“. Letztere ist besonders wichtig, damit Sie ihre eigenen verschlüsselten Emails wieder entschlüsseln und damit lesen können.

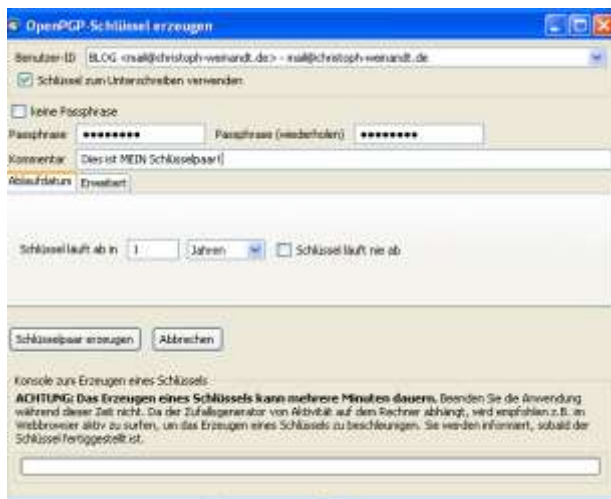
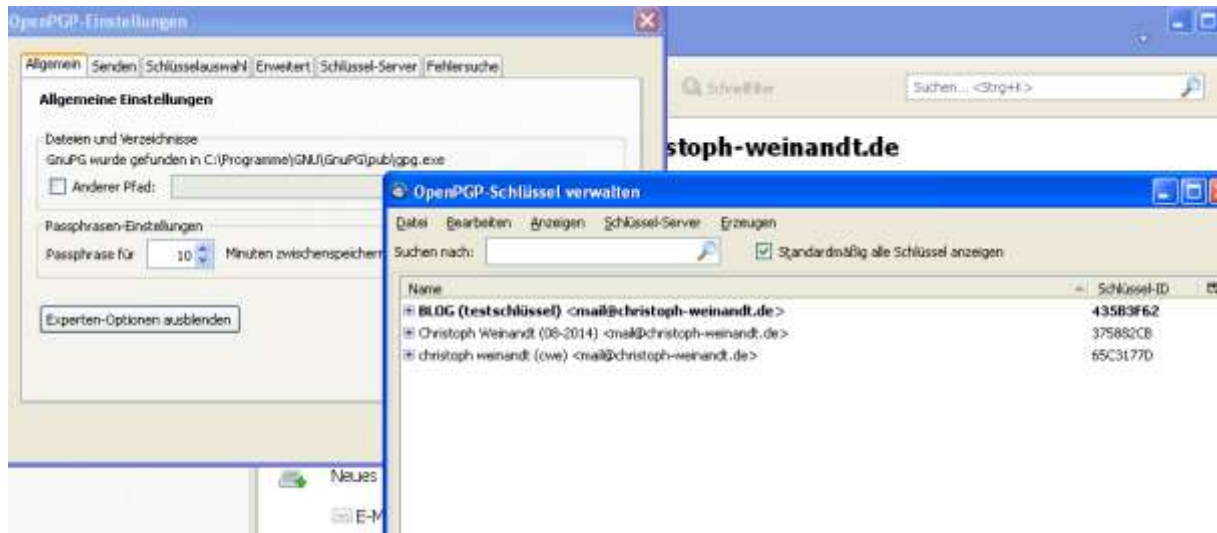
Wenn Sie nun soweit sind, fangen wir an, Ihr Schlüsselpaar zu erzeugen.

Schlüsselpaar erzeugen

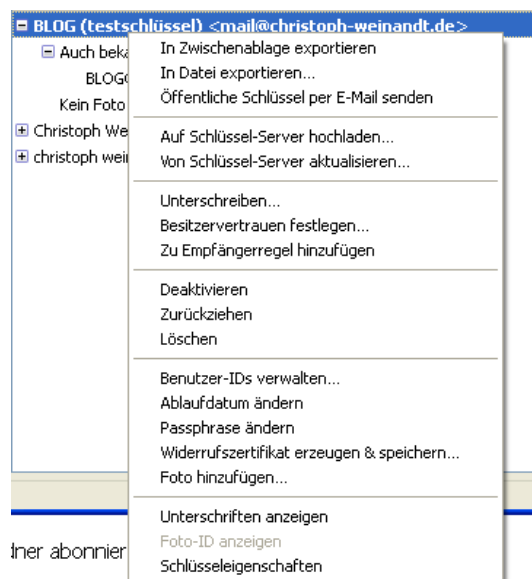
Damit Sie Emails verschlüsseln können, benötigen Sie einen Schlüssel. Dieser besteht aus zwei Teilen, da es sich um eine asymmetrische Verschlüsselung handelt. Der PRIVATE Schlüssel ist IHR Schlüssel und auf den müssen Sie gut aufpassen, denn er dient zum ENTSCHLÜSSELN. Der ÖFFENTLICHE Schlüssel wird an jeden weitergegeben, dem Sie eine verschlüsselte Mail schicken wollen und dient zum VERSCHLÜSSELN. Das ganze ist ein sog. Schlüsselpaar. Wenn Sie jemandem eine verschlüsselte Email schicken wollen, benötigen Sie dazu seinen ÖFFENTLICHEN Schlüssel. Sie können diesen manuell in das Thunderbird Addon importieren oder den öffentlichen Schlüssel automatisch von einem Keyserver herunterladen.

Zum Erzeugen Ihres eigenen Schlüsselpaares gehen Sie auf die Schlüsselverwaltung:

Dort können Sie im Menu „Erzeugen“ ihr Schlüsselpaar erzeugen:



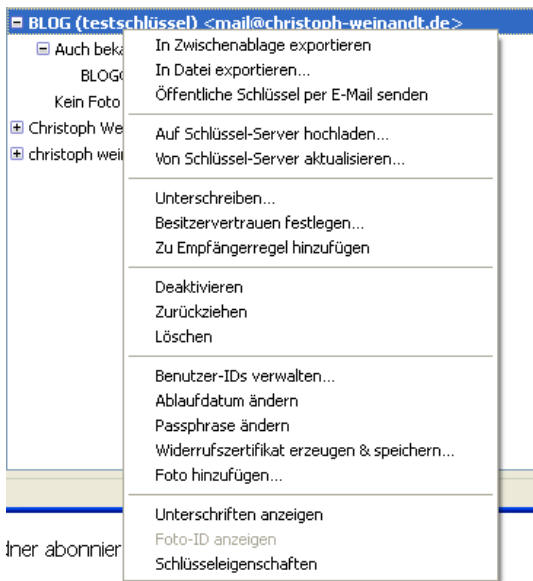
Es ist empfehlenswert, die Gültigkeit auf ein Jahr zu begrenzen und den privaten Schlüssel zusätzlich mit einem Passwort zu sichern.



Unter „Erweitert“ können Sie die Schlüssellänge und den Algorithmus bestimmen – die Voreinstellungen (RAS, 2048 bit) können Sie getrost übernehmen.

Danach dauert es je nach Leistung Ihres Systems eine Weile, bis die Erstellung des Schlüsselpaares abgeschlossen ist. Dann werden Sie nach der Erstellung eines sog. „Widerrufszertifikates“ gefragt

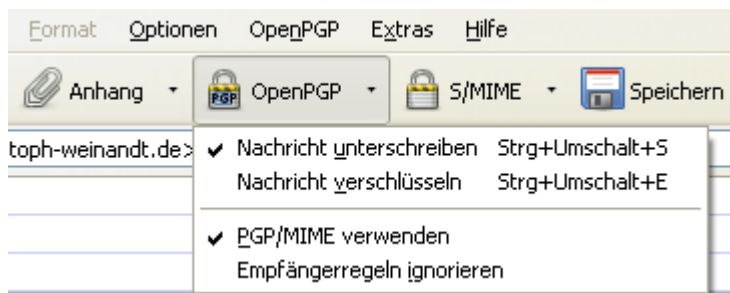
– dies bitte UNBEDINGT tun, denn nur so können Sie vor Ablauf der Gültigkeit Ihren öffentlichen Schlüssel zurückziehen



Damit ist der wesentliche Teil schon abgeschlossen – Sie haben damit eigentlich alles, um zu verschlüsseln. Jetzt sollten Sie Ihren öffentlichen Schlüssel noch auf einen der Keyserver hochladen – diese sind vorkonfiguriert. Mittels rechtsklick auf Ihren gerade erstellen Schlüssel erreichen Sie das abgebildete Menü und können dort den Eintrag „auf schlüsselsever hochladen“ auswählen.

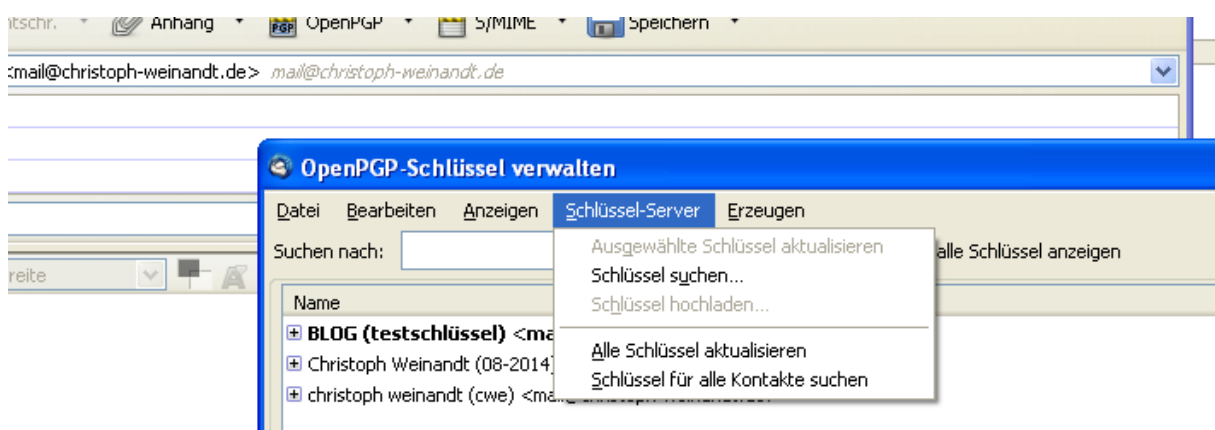
Email versenden

Sie können sowohl signieren als auch verschlüsseln – dazu schreiben Sie in Thunderbird eine Email und wählen dann im Menü aus, ob Sie nur signieren oder auch verschlüsseln wollen. Sobald Sie auf



senden klicken, werden Sie aufgefordert, Ihr Passwort für Ihr Schlüsselpaar einzugeben – wenn Sie an jemanden eine Mail nur signieren, dann brauchen Sie nichts weiter als „Nachricht unterschreiben“ auszuwählen. Wollen Sie dagegen auch die „Nachricht verschlüsseln“ MUSS der

öffentliche Schlüssel des Empfängers Ihnen zugänglich sein. Dazu suchen Sie entweder manuell auf dem Keyserver nach der Emailadresse des Empfängers, indem Sie die Schlüsselverwaltung nutzen:



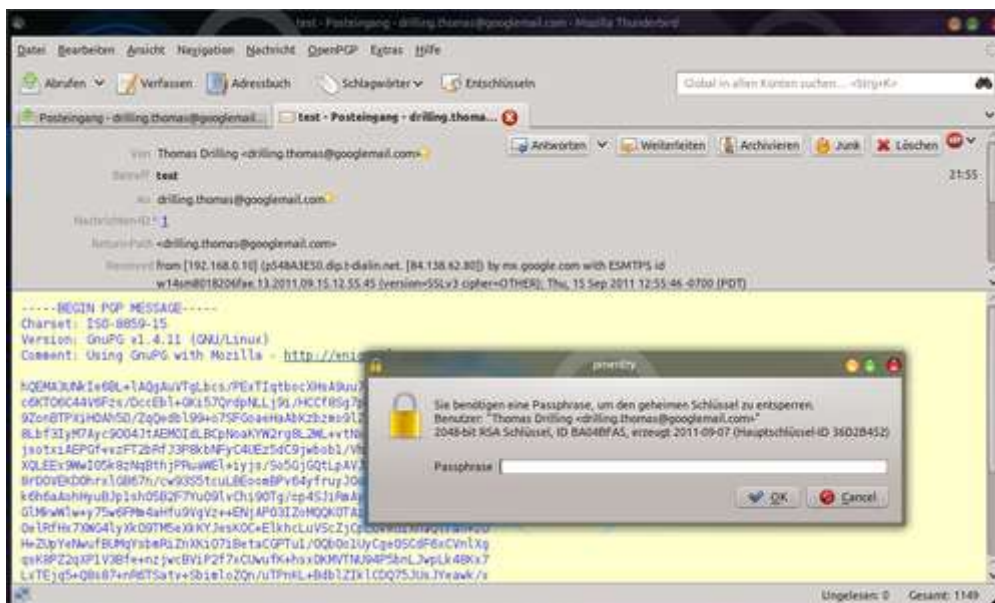
Oder Sie überlassen dies dem Programm selbst. Haben Sie den öffentlichen Schlüssel einmal auf diesem (oder einem anderen Weg) importiert, können Sie auch mit dem Empfänger verschlüsseln.

Email empfangen

Wenn Sie eine signierte Email empfangen, wird die Signatur automatisch geprüft und Sie sehen dies in einem kleinen Fenster der Emailvorschau:



Wenn die Mail, die Sie erhalten, verschlüsselt ist, wird diese automatisch entschlüsselt und Sie werden nach dem Passwort Ihres Schlüsselpaares gefragt:



Sie sehen, es ist gar nicht kompliziert:

1. Installation Enigmail und Thunderbird
2. Emailkonto einrichten
3. Schlüsselpaar erstellen
4. eigenen öffentlichen Schlüssel auf einen Keyserver hochladen
5. öffentlichen Schlüssel der/des Mailempfängers besorgen
6. **Verschlüsseln!**

Weitere Informationen gibt es im Netz und bei mir.

mail@christoph-weinandt.de