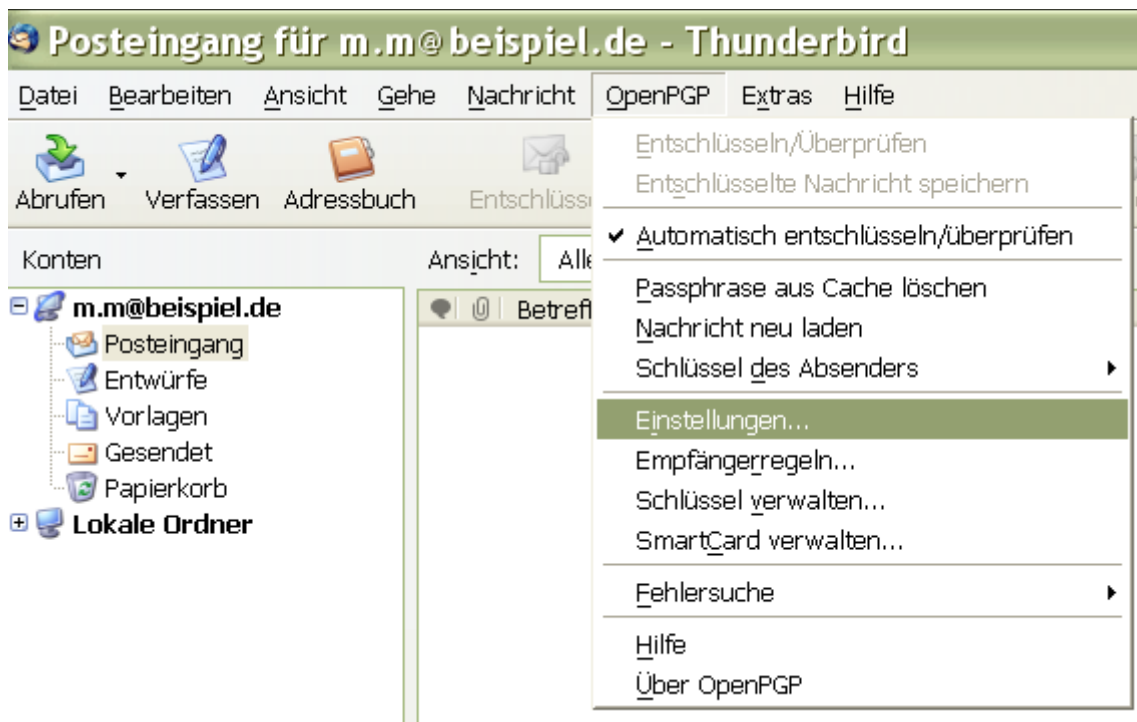
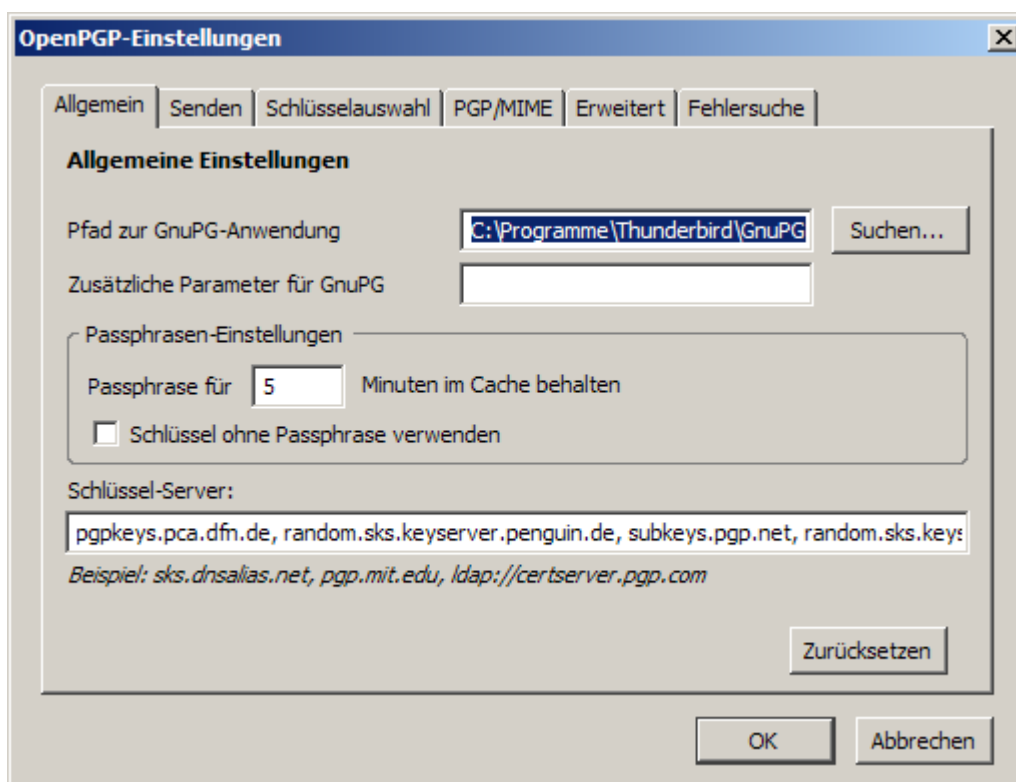


Verschlüsselung und Signatur mit Enigmail

Wie Sie sicherlich bemerkt haben, ist nach dem Neustart von Thunderbird in der Taskleiste ein neuer Eintrag namens "Open PGP" entstanden. Klicken Sie diesen an und wählen im aufklappenden Menü "Einstellungen".



Es öffnet sich ein Fenster, in dem Sie lediglich bei zwei Einstellungen etwas verändern müssen. Bei der Einstellung, wie lang ihr Passphrase im Cache (Speicher) bleiben soll, geben Sie eine Zahl zwischen 45 und 60 Minuten ein. Dies ist eine sinnvolle Zeitangabe. Schließen Sie nun dieses Fenster mit **OK**.



Erstellung ihres eigenen Schlüssels

Da ihr Thunderbird nun in der Lage ist Emails zu verschlüsseln, benötigen Sie eigentlich nur noch einen eigenen Schlüssel, mit dem Sie anderen Leuten ihre Identität bestätigen. Wählen Sie wieder in der Taskleiste "Open PGP" und anschließend "Schlüssel verwalten".



Um nun ihren eigenen Schlüssel zu erstellen, wählen Sie im sich öffnenden Fenster "Erzeugen" und dann "Neues Schlüsselpaar...".



Es öffnet ein sich Fenster mit dem Sie nun ihren Schlüssel erstellen können. Dazu wählen Sie als Benutzer-ID ihre Emailadresse aus und setzen einen Haken bei "Schlüssel zum Unterschreiben verwenden". Bei Passphrase müssen Sie einen Satz eingeben, an den Sie sich gut erinnern können, den aber auch nur Sie wissen, da es sich um so etwas wie eine PIN-Nummer wie etwa bei ihrer EC-Karte handelt. Geben Sie den Passphrase zweimal ein und setzen Sie einen Haken bei "Schlüssel läuft niemals ab". Die Schlüsselstärke können Sie gerne verändern, aber 2048 ist ein wirklich gutes Maß. Wenn Sie mit allen Eingaben fertig sind, können Sie die Schlüsselpaarerstellung mit einem Klick darauf starten.

OpenPGP-Schlüssel erzeugen

Benutzer-ID: Max Mustermann <m.m@beispiel.de> - m.m@beispiel.de

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase: Passphrase wiederholen:

Kommentar:

Ablauf-Datum: **Erweitert**

Schlüssel läuft ab in: 5 Jahren Schlüssel läuft nie ab

Schlüsselpaar erzeugen Abbrechen

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.

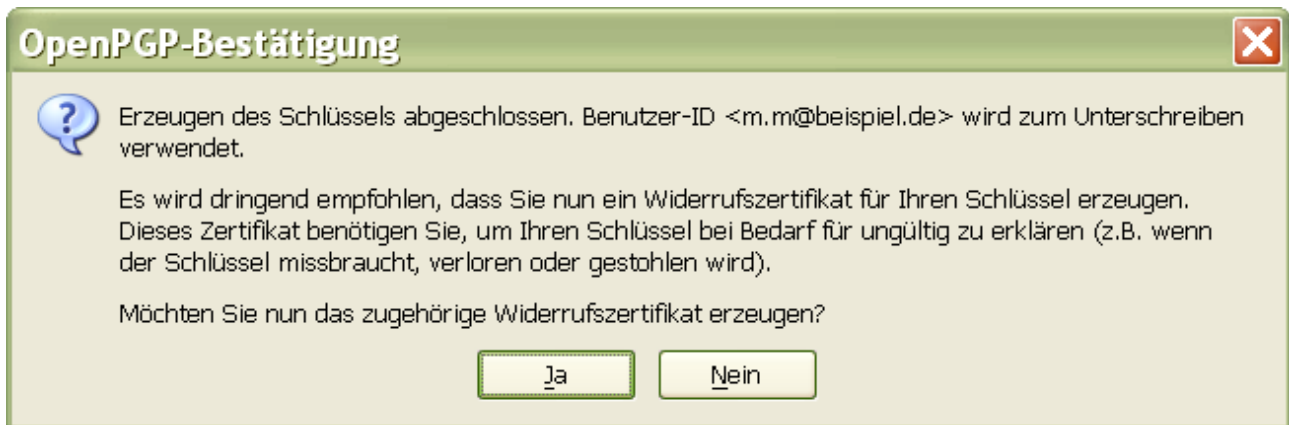
Sie werden nun gefragt, ob ein öffentlicher und ein privater Schlüssel erstellt werden soll. Beantworten Sie dies mit **Ja**. Nun dauert es einige Zeit bis ihr Schlüssel erstellt ist.

OpenPGP-Bestätigung

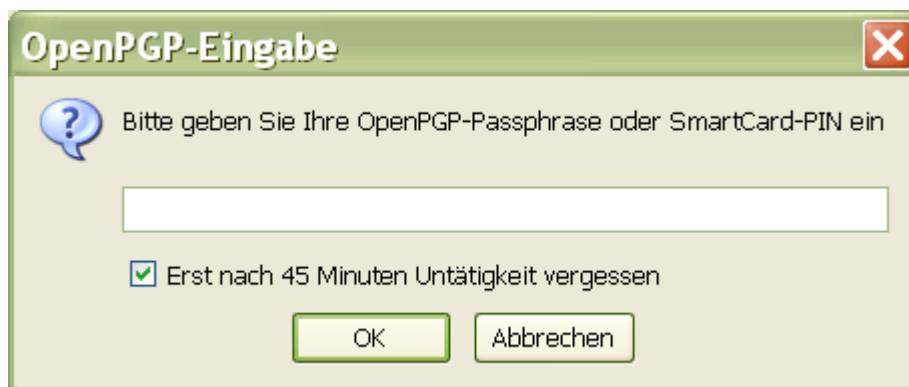
Erzeuge öffentlichen und privaten Schlüssel für 'Max Mustermann <m.m@beispiel.de>?'

Ja Nein

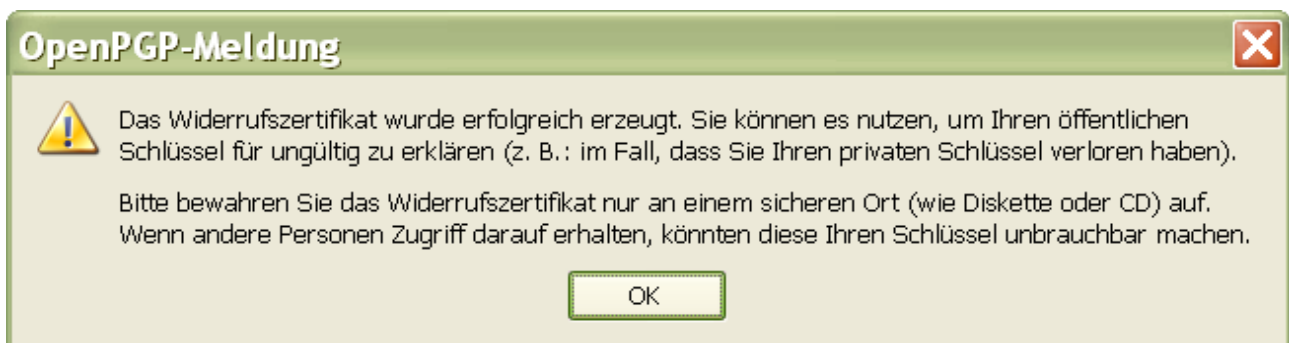
Danach erscheint folgende Meldung, die Sie mit **Ja** bestätigen.



Da ihr Schlüssel jetzt eigentlich fertig ist, will Enigmail, dass Sie ihren Passphrase ein erstes Mal eingeben und mit **OK** beenden. Sobald dies geschehen ist, öffnet sich ein Fenster, mit dem Sie ein Widerrufs-zertifikat ihres soeben erstellten Schlüssel abspeichern können. Dies tun Sie am besten in eigene Dateien in einem Unterordner für alle ihre Schlüssel.



Als letzter Schritt folgt noch eine Meldung das ihre Schlüsselerzeugung erfolgreich war. Diese schließen Sie mit **OK**. Herzlichen Glückwunsch, Sie haben von nun an einen Schlüssel, mit dem Sie ihre Emails verschlüsseln können.



Hochladen des öffentlichen Schlüssels

Damit Freunde und Kollegen Ihnen eine verschlüsselte Email zukommen lassen können, benötigt der Absender einer zu verschlüsselnden Email Ihren öffentlichen Schlüssel. Für die zentrale Verwaltung öffentlicher Schlüssel gibt Schlüsselsever im Internet.

Zuerst markieren Sie ihren eben erstellten Schlüssel, wählen über „Schlüssel-Server“ und danach im aufklappenden Menü den Eintrag „Schlüssel hochladen ...“.



Nachdem sie die Abfrage des Schlüssel-Servers mit **OK** bestätigen wird Ihr öffentliche Schlüssel hochgeladen. Nach kurzer Zeit steht Ihr öffentlicher Schlüssel zur Verfügung. Nun kann ihr Kommunikationspartner ihren Schlüssel in sein Email-Programm importieren und Ihnen eine verschlüsselte Email zuschicken.

Importieren anderer Schlüssel

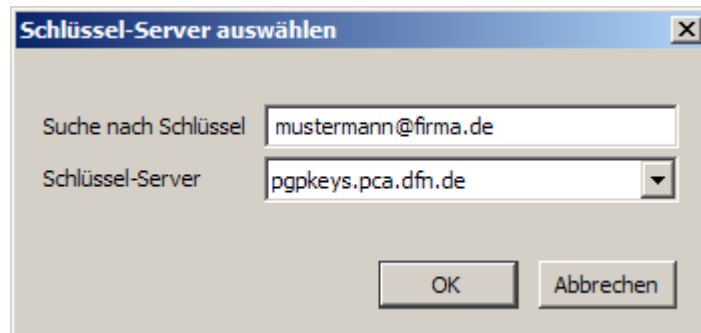
Nachdem Sie gerade eben ihren eigenen Schlüssel erzeugt und veröffentlicht haben, benötigen Sie ja außerdem noch die Schlüssel ihrer Freunde und Kollegen, damit Sie die Emails, die Sie erhalten, den Absender genau identifizieren können. Fragen Sie ihre Freunde nach den Schlüsseln oder laden Sie sich die Schlüssel aus dem Internet von einem Schlüssel-Server.

Was Sie dann damit anfangen, sehen Sie im nun folgenden Abschnitt:

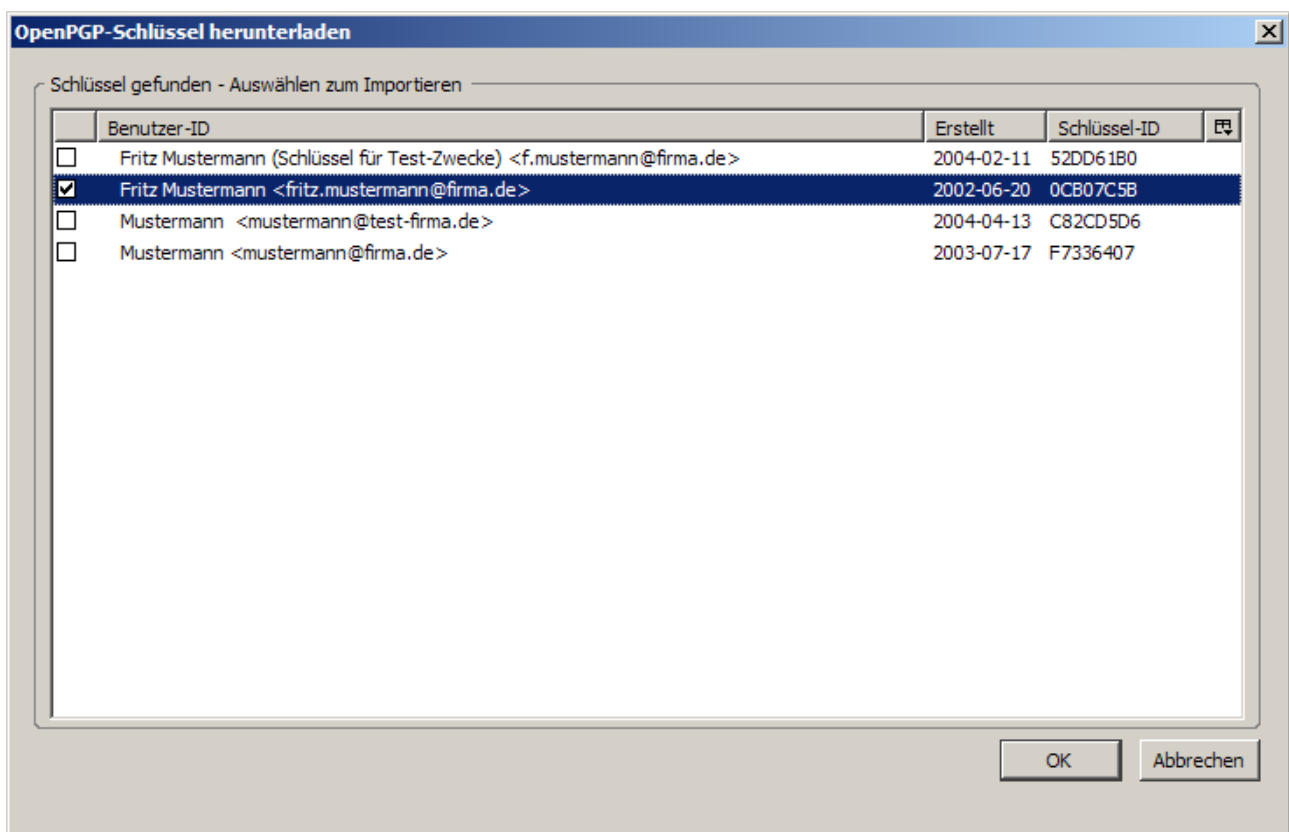
Falls die OpenPGP-Schlüsselverwaltung nicht bereits offen ist, öffnen Sie sie, wie im vorherigen Abschnitt beschrieben. Zu Zeit steht nur ihr eigener Schlüssel in der Verwaltung.



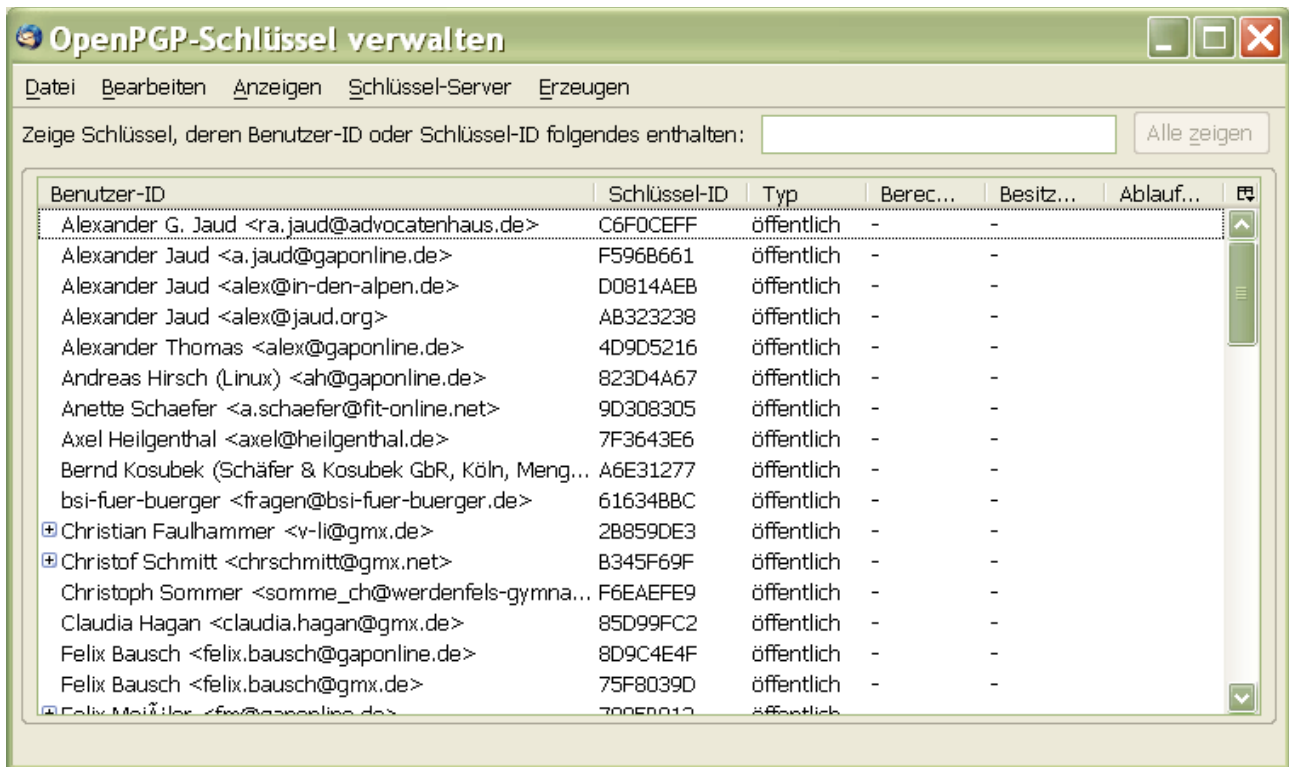
Um nun einen Schlüssel vom Schlüsselserver zu importieren wählen Sie „Schlüssel-Server“ und im aufklappenden Menü „Schlüssel suchen“. Im Feld „Suche nach Schlüssel“ geben Sie vorzugsweise die Email-Adresse des Schlüssel-Inhabers ein



Durch bestätigen mit **OK** startet die Suchanfrage auf dem Schlüsselserver. Nun öffnet sich ein Fenster, mit dem Sie ihre heruntergeladenen Schlüssel auswählen müssen.



Nach dem Sie mit **OK** die Auswahl quittiert haben erscheinen alle Schlüssel die Sie soeben importiert haben, sowie ihr eigener in der Schlüsselverwaltung. Als abschließenden Punkt müssen Sie die Schlüssel noch unterschreiben und je nach Person auch die Vertrauenswürdigkeit des Schlüssels festlegen. Klicken Sie dazu rechts auf einen der Schlüssel und wählen dann "Unterschreiben". Im sich öffnenden Fenster klicken Sie "Ich habe es sehr genau geprüft" und fahren dann mit **OK** fort. Sie müssen nun ihren Passphrase eingeben und dann mit **OK** abschließen. Sie haben den Schlüssel damit unterschrieben. Falls der Besitzer des Schlüssels bereits einige ihrer Schlüssel hat und Sie schon unterschrieben hat, wird dies automatisch übernommen, um ihnen die Arbeit zu erleichtern.



Hiermit ist die Installation und Einstellung der Verschlüsselung ihrer Emails beendet. Sie können nun ihre Mails sicher verschlüsseln, bzw. nur unterschreiben, um ihre Identität zu bestätigen.