Installation und Konfiguration von Thunderbird in Kombination mit Enigmail

Inhaltsverzeichnis

Autor: Toni Müller

Stand: 13.07.2009

Lizenzbestimmungen

Zielsetzung

Das Ziel dieser Anleitung ist es, Ihnen die Grundlagen der Email-Verschlüsselung zu erläutern und Ihnen zu einer sinnvoll konfigurierten Kombination aus Thunderbird, GnuPG und Enigmail zu verhelfen, mit der Sie

diese Combo im Alltag ohne Probleme benutzen können.

Umfang

In dieser Anleitung wird die Installation und Konfiguration von Enigmail, sowie die Generierung eines Schlüssels und das Versenden sowie der Empfang einer verschlüsselten Nachricht beschrieben.

Voraussetzungen

Wir setzen voraus, daß Sie Thunderbird Version 2.x und GnuPG installiert haben. Außerdem wird vorausgesetzt, daß Sie auf Ihrem Computer keine Probleme mit Viren oder Trojanern haben, sondern ziemlich sicher sind, daß Ihr Computer frei von Schadsoftware ist. Eine Konfiguration mit Outlook oder Outlook Express wird nicht beschrieben, da diese beiden Programme fast nicht dazu zu bewegen sind, mit OpenPGP oder PGP überhaupt zusammenzuarbeiten. Dem Hersteller sei es gedankt, und den Anwendern ein Wechsel auf andere Emailprogramme, die solche Probleme nicht haben, empfohlen.

Grundlagen der Email-Verschlüsselung

Begriffsbestimmung

Email-Verschlüsselung bedeutet heutzutage die Anwendung sogenannter asymmetrischer Kryptographie. Diese Verfahren sind weltweit als die sichersten, allgemein verfügbaren Methoden etabliert. Bei asymmetrischer Verschlüsselung benutzt man einen zweiteiligen Schlüssel (allgemein als „Schlüsselpaar“ bezeichnet). Der eine Teil ist der **private Schlüssel**. Diesen sollte man **unter allen Umständen geheim** halten, denn wer diesen Schlüssel besitzt, kann sich, wenn auch vielleicht nicht ganz einfach, als Sie ausgeben, also Ihre Identität annehmen. Der andere Teil ist der öffentliche Schlüssel, der dazu gedacht ist, an Ihre Kommunikationspartner, oder einfach weltweit, verteilt zu werden.

Es gibt zwei heutzutage eingesetzte Verschlüsselungsverfahren, die jeweils eigene Vor- und Nachteile haben. Das eine Verfahren heißt „S/MIME“ und wird ohne Erweiterungen von vielen Emailprogrammen unterstützt. Aufgrund gewisser Nebenwirkungen dieses Verfahrens, etwa der unflexiblen Handhabung und der zwangsweise zentralisierten Zertifikatsverwaltung („X.509-Zertifikate“), ist dieses Verfahren im Internet nicht oft anzutreffen. Der andere, wesentlich populärere und leistungsfähigere Standard heißt „OpenPGP“. Dieses Verfahren wird im Internet sehr breit eingesetzt, von der Signatur und Verschlüsselung von Emails, wo das Verfahren zuerst eingesetzt wurde, bis hin zur Signatur von Softwarepaketen oder Webseiten.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

Verfahrensübersicht

Einrichtung

Die beteiligten Kommunikationspartner, also z.B. Sie und jemand, mit dem Sie verschlüsselte Emails austauschen wollen, benötigen neben der passenden Software jeweils ein Schlüsselpaar, wie oben beschrieben. Außerdem benötigt jeder den **öffentlichen** Schlüssel seines Gegenübers. Die Verteilung der öffentlichen Schlüssel kann man durch sogenannte Keyserver erledigen lassen, wie weiter unten gezeigt wird. Keyserver sind Computer im Internet, die meistens Teil eines („des“) Keyserver-Netzwerkes sind, wo man seinen öffentlichen Schlüssel hochladen kann. Die Schlüssel werden dann automatisch auf alle Server in dem Netzwerk kopiert, so daß sie im Idealfall weltweit und mit hoher Fehlertoleranz abrufbar sind.

Nutzung (Übersicht)

Wie läuft nun die verschlüsselte Kommunikation in groben Zügen ab, nachdem das Schlüsselaustauschproblem gelöst ist? Betrachten wir zuerst das Versenden einer Email:

1. Sie schreiben eine Email.
2. Sie wählen die Option „Email verschlüsseln“ aus.
3. Das Verschlüsselungsprogramm „findet“ für Sie die Schlüssel, die zu dem angegebenen Empfänger passen.
4. Sie wählen einen Schlüssel aus der Liste aus.
5. (optional, aber üblich und empfohlen) Sie signieren Ihre Email, indem Sie eine Art Paßwort in einem Dialogfenster eingeben.
6. Die Email wird ganz normal von Ihrem Emailprogramm abgeschickt.

Analog verhält es sich mit dem Empfang einer verschlüsselten Nachricht:

1. Sie erhalten eine verschlüsselte Email. die von dem Emailprogramm schon als solche erkannt wird.
2. Sie klicken die Nachricht an, um sie zu lesen.
3. Das Programm fragt Sie nach Ihrem Paßwort, um Ihren privaten Schlüssel zu „entsichern“.
4. Sie geben das Paßwort ein und bestätigen.
5. Die Email wird angezeigt.

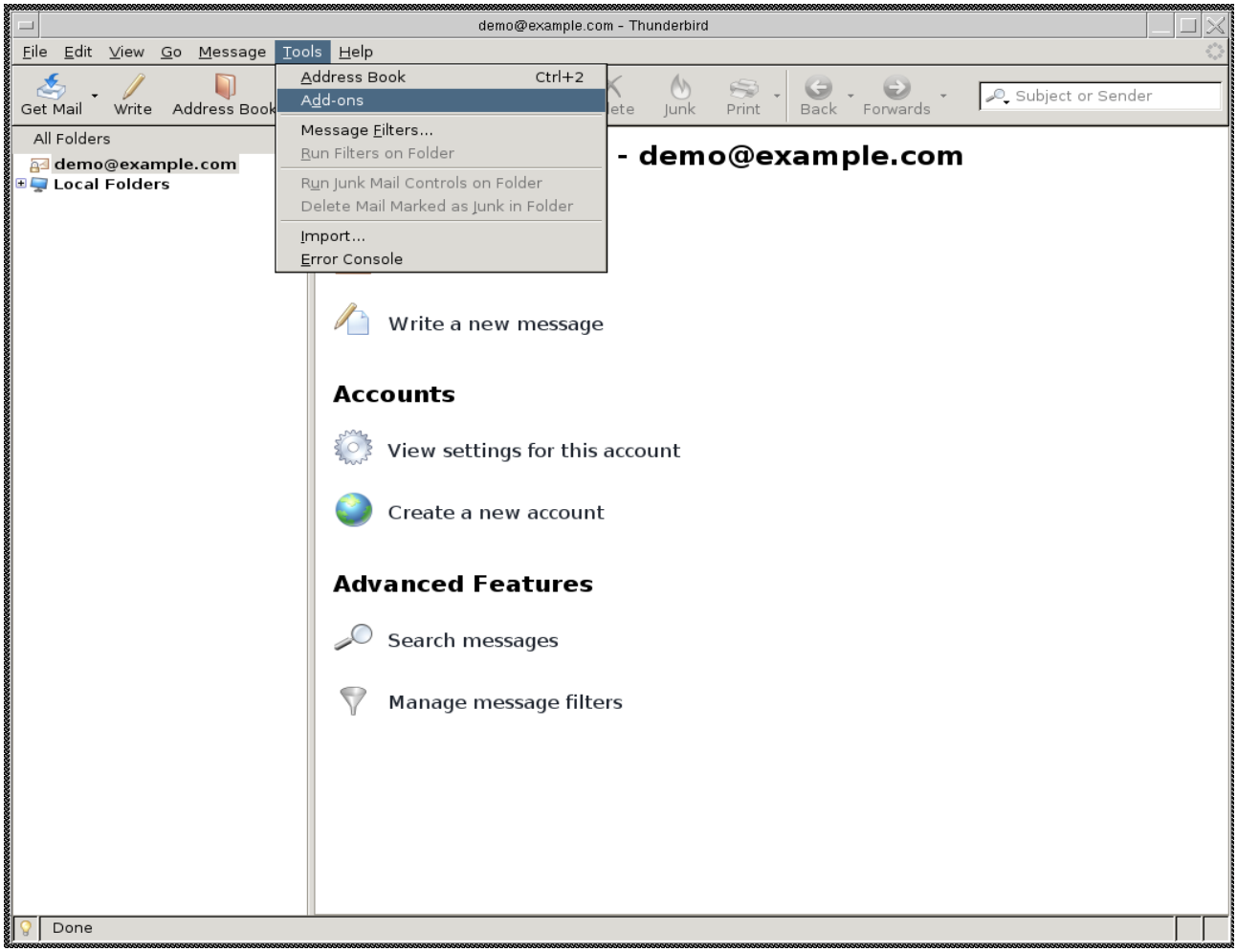
Falls die Email zusätzlich signiert war (siehe Schritt 5. unter Versand), wird Ihnen angezeigt, mit wessen Schlüssel die Nachricht unterschrieben ist, und wann die Nachricht unterschrieben wurde.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

Installation von Enigmail

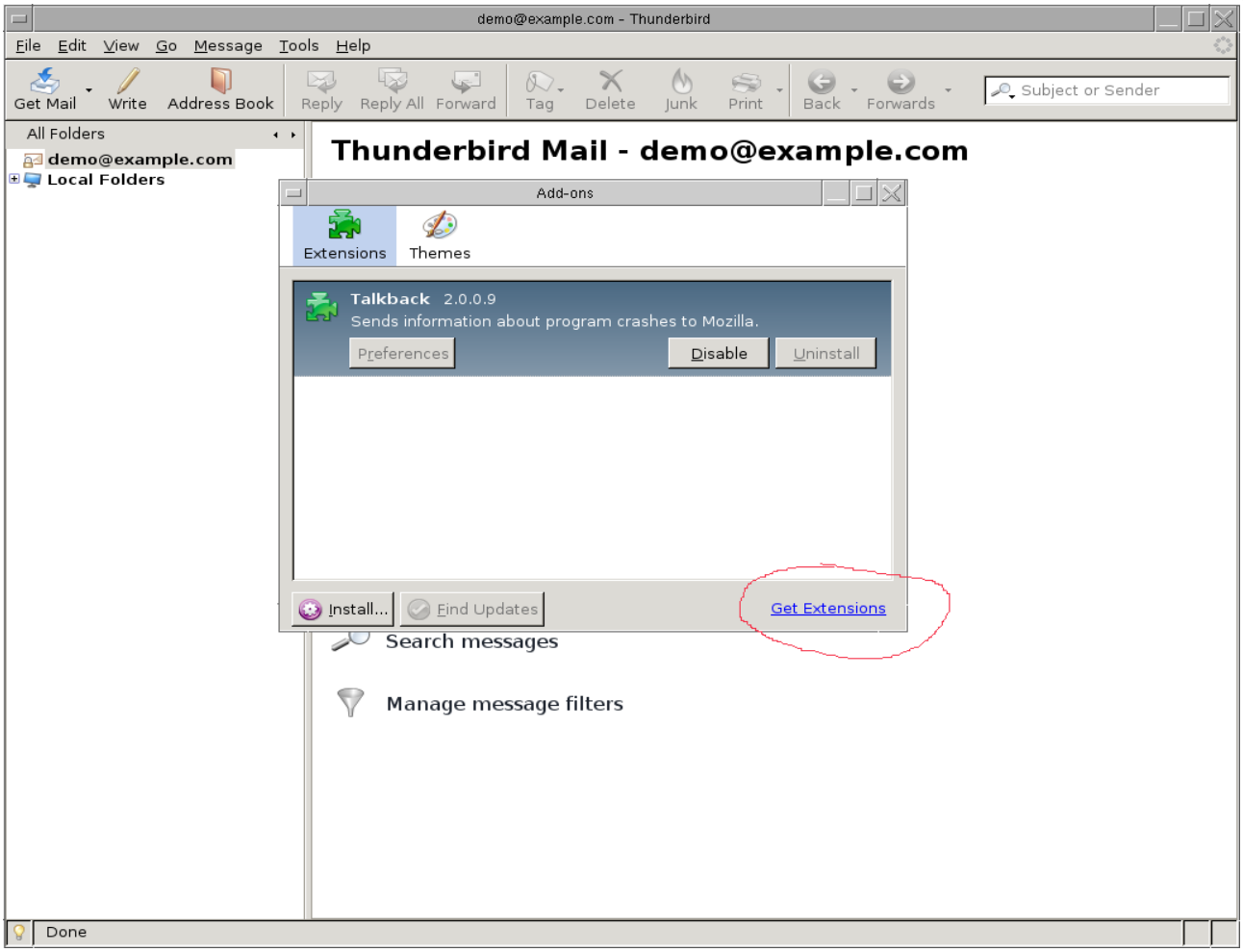
Sie wollen die Erweiterung „Enigmail“ installieren, um GnuPG mit Thunderbird zu integrieren. Dies ist nicht zwingend erfoderlich - Sie können beide Programme auch einzeln benutzen - aber es ist äußerst sinnvoll, um eine akzeptable Benutzbarkeit zu erzielen.

Da Thunderbird keine eigene Möglichkeit hat, eine Webseite aufzurufen, die Erweiterungen aber, wie bei Mozilla üblich, über eine Webseite verteilt werden, lassen Sie sich von Thunderbird zuerst zu der Webseite leiten, wo diese Erweiterungen katalogisiert sind. Dazu öffnen Sie den Dialog für die Verwaltung der Erweiterungen:



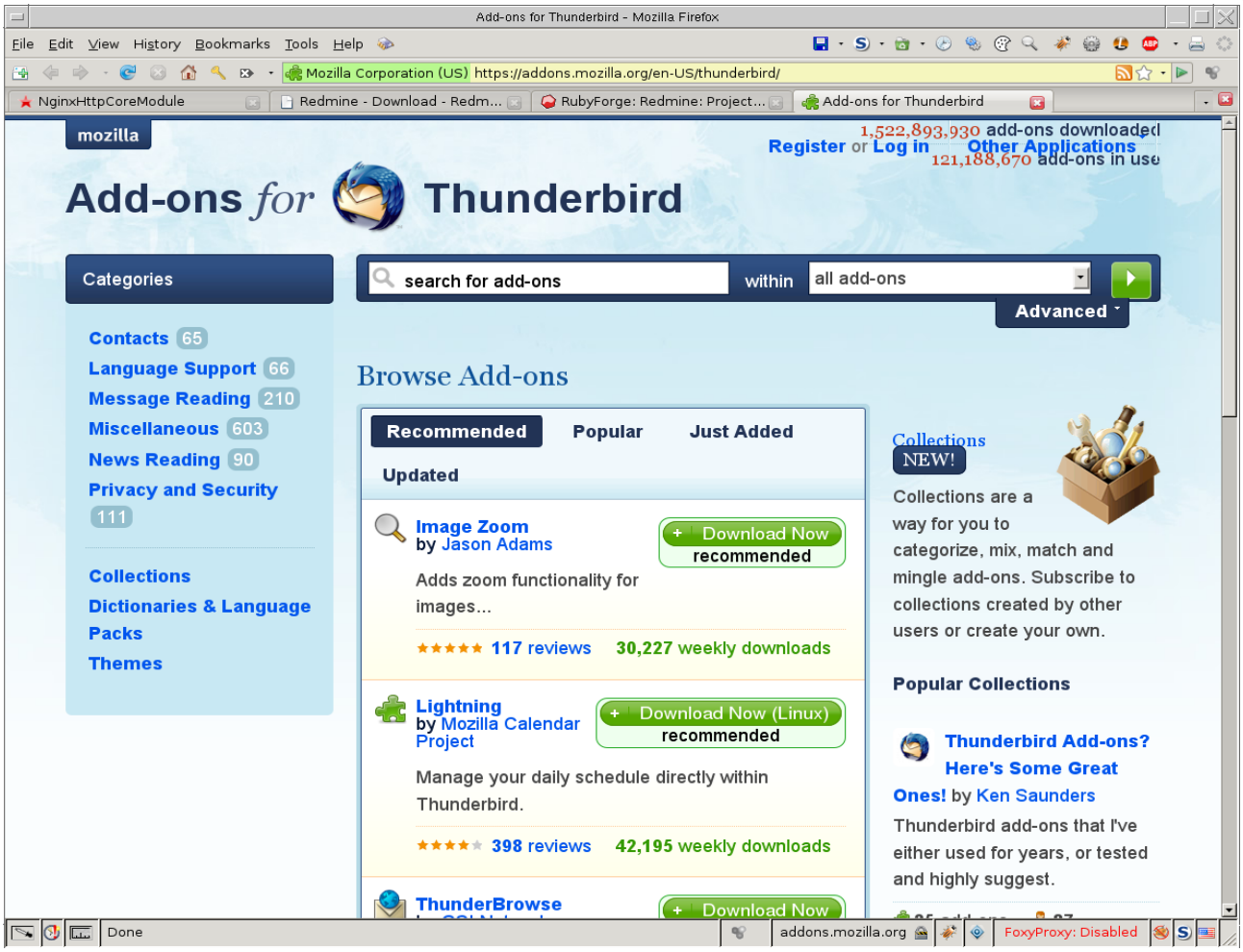
Sie bekommen die installierten Erweiterungen und einen Link, um solche herunterzuladen, angezeigt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



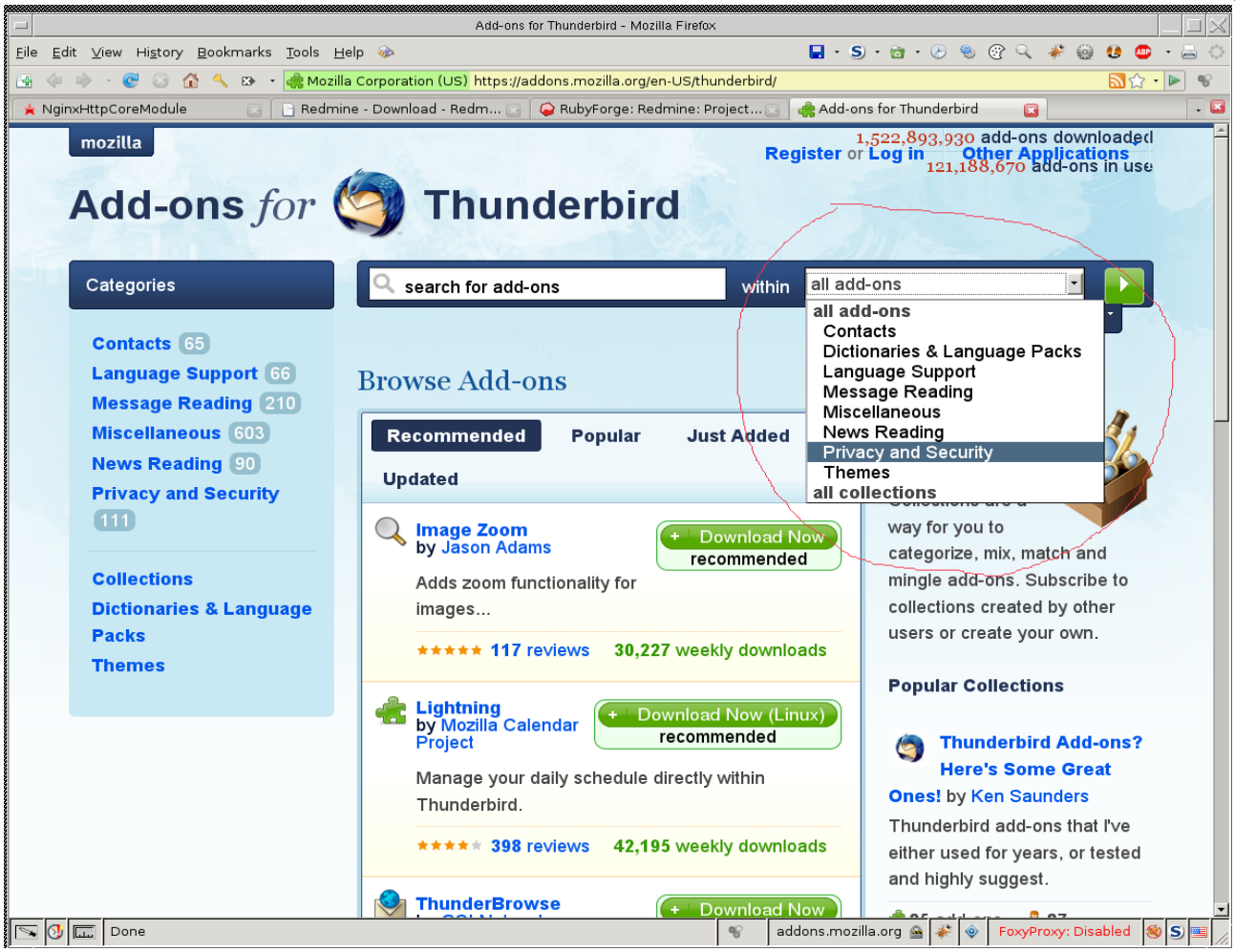
Wenn Sie hier auf „Get Extensions“ (oder wie das auf deutsch heißt) klicken, öffnet sich ein Browserfenster mit einer Liste der Erweiterungen:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



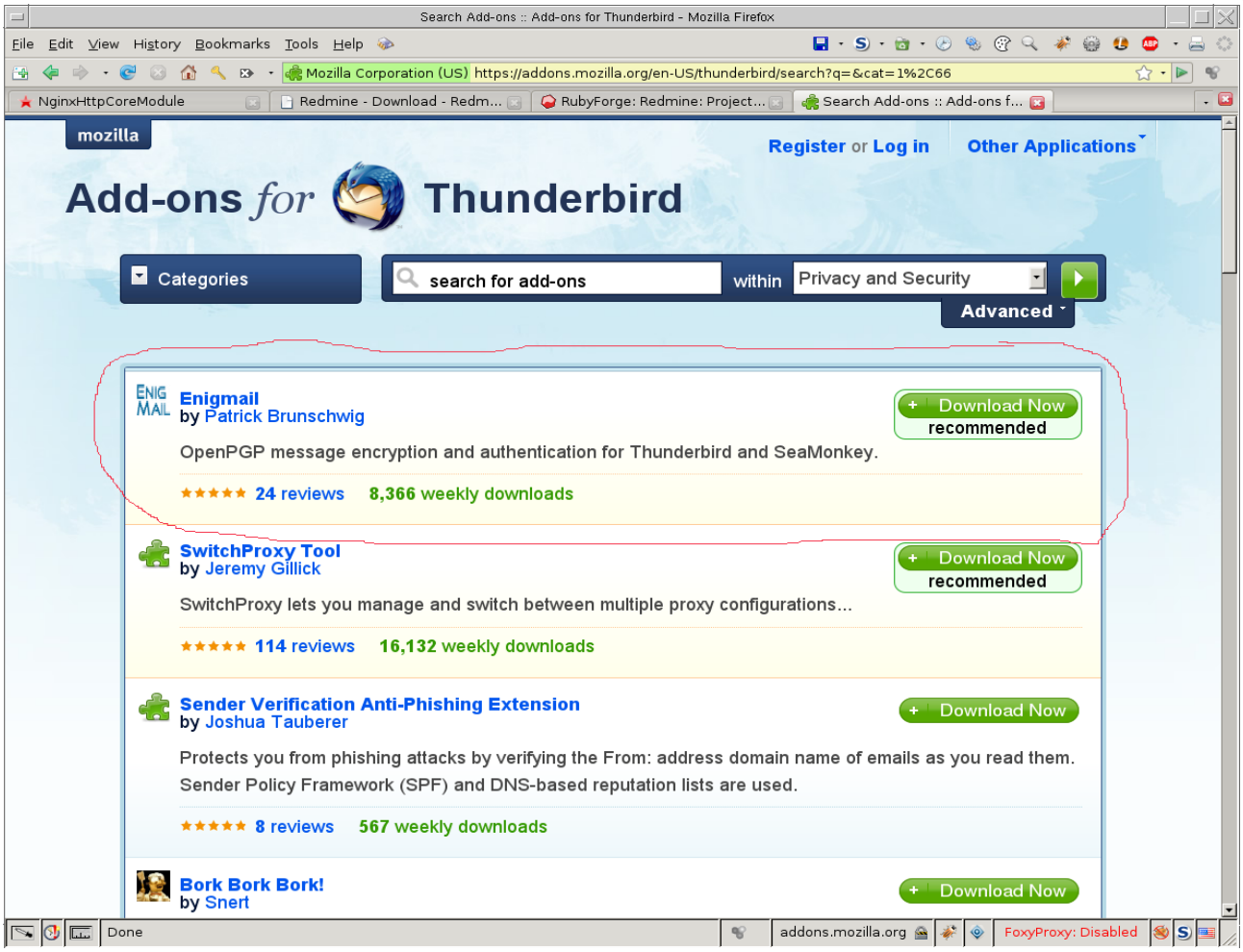
Nun suchen Sie die Erweiterung „Enigmail“. Die Erweiterungen sind nach Funktionsbereichen gruppiert. Man erwartet „Enigmail“ in der Gruppe „Privatsphäre und Sicherheit“, oder, was unten zu sehen ist, „Privacy and Security“, was die englische Übersetzung dieser Begriffe darstellt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

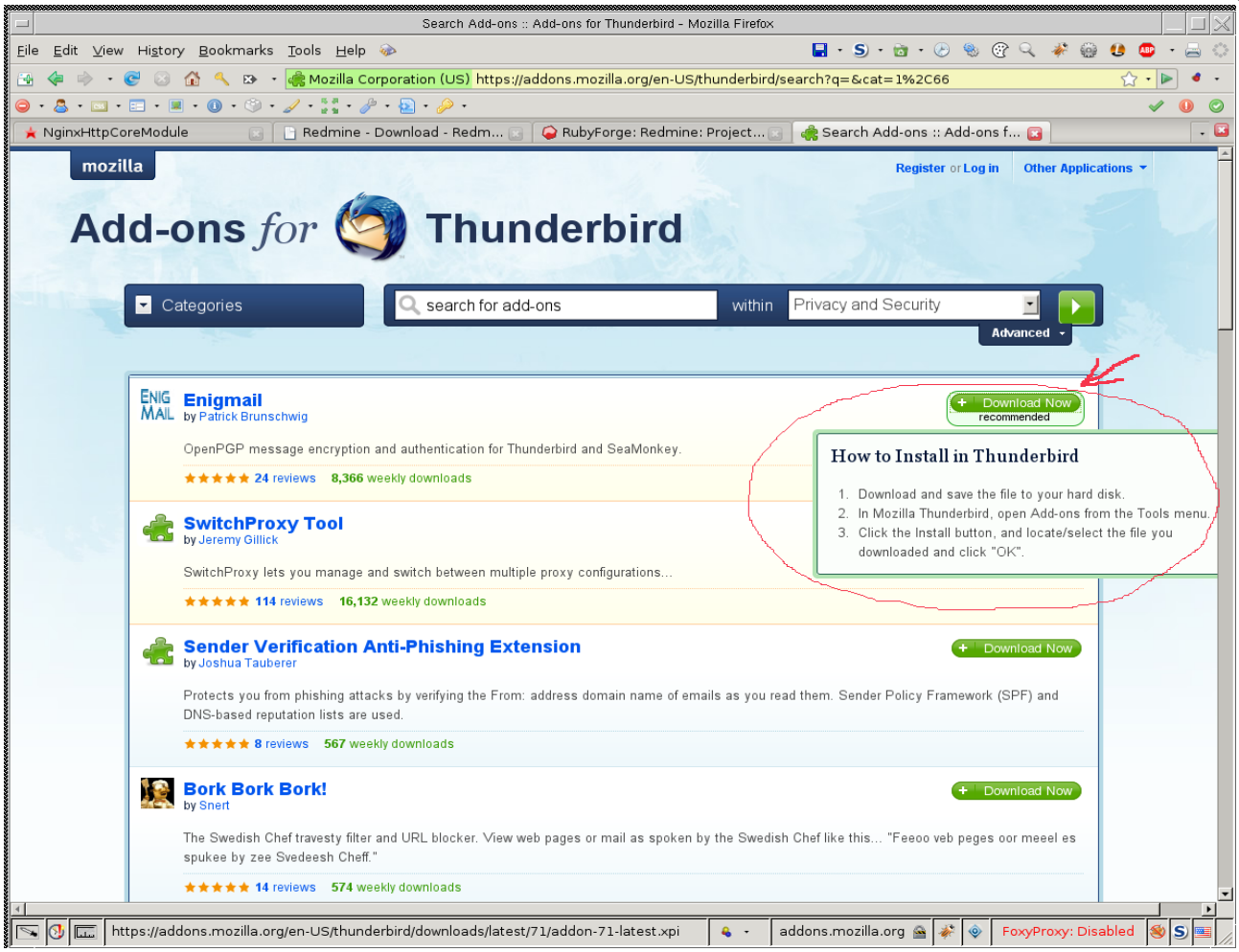


Sie wählen diese Gruppe aus, um die Suche in der Vielzahl der Erweiterungen zu erleichtern:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

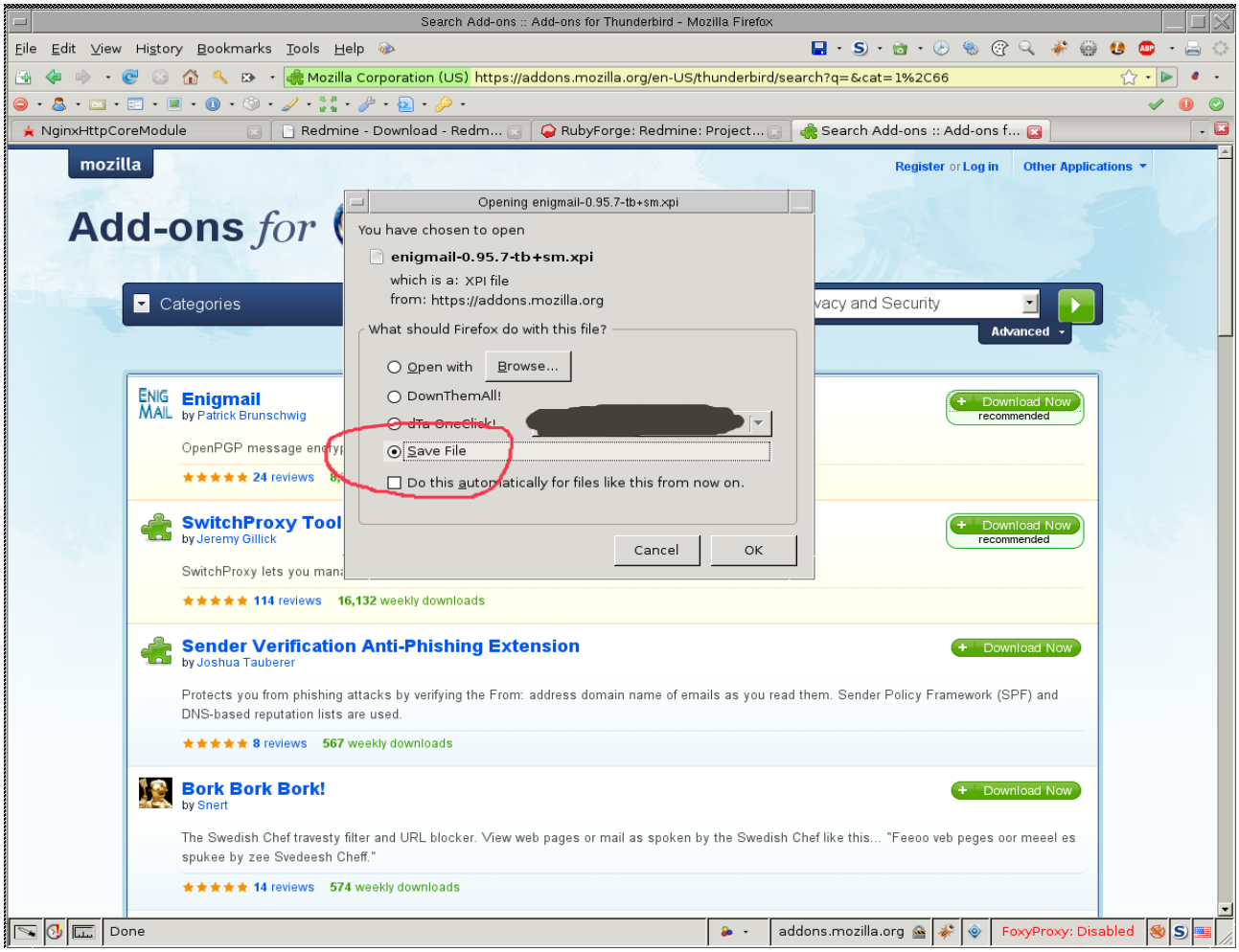


Enigmail wird bereits als erster Treffer angezeigt. Sie laden die Erweiterung herunter und sehen dabei eine kurze Installationsanleitung:



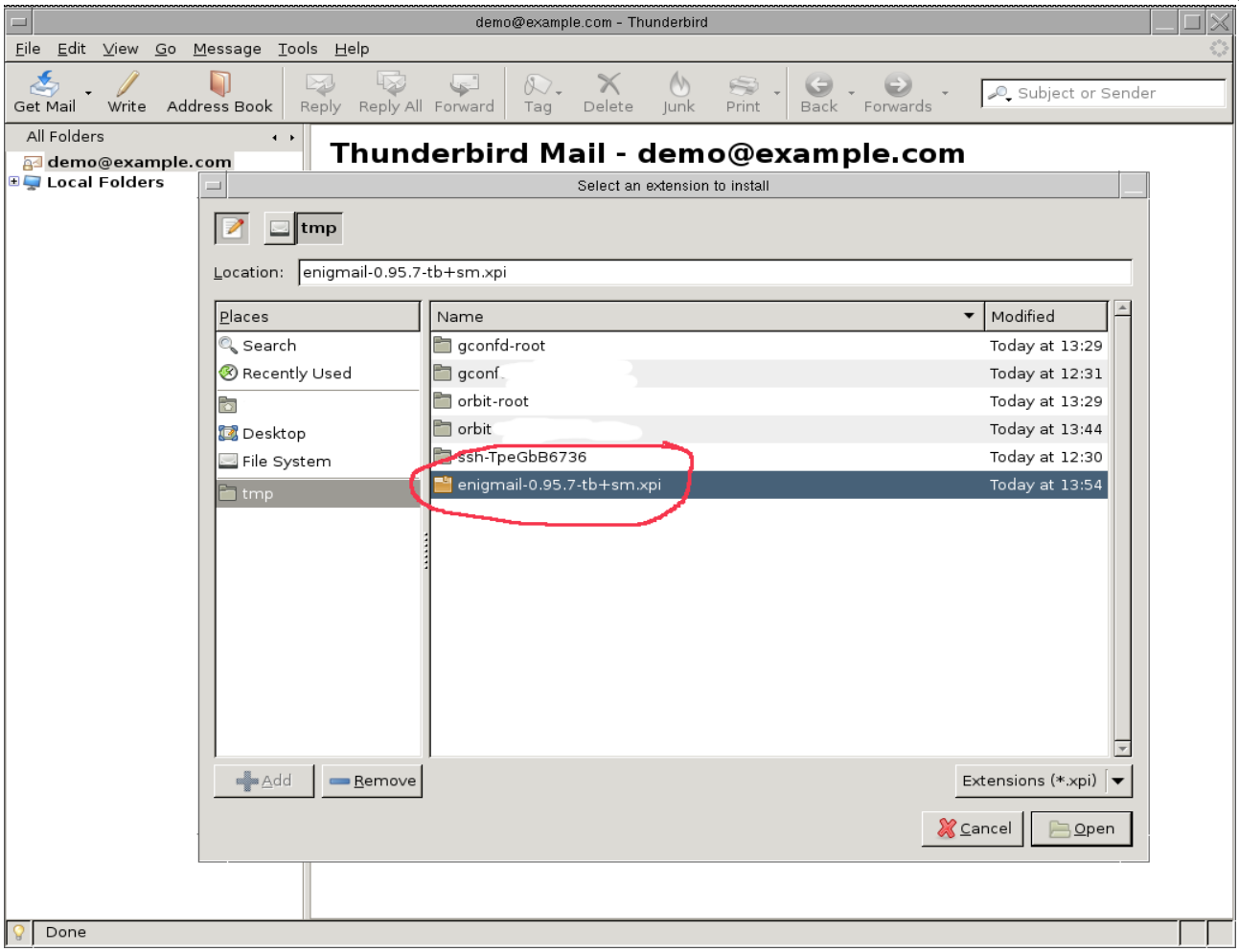
Sie speichern die Erweiterung auf Ihrer Festplatte, um sie später von Thunderbird aus installieren zu können. In dem zweiten Bild weiter oben ist auf der linken Seite neben „Get Extensions“ ein Knopf „Installieren...“ zu sehen. Wenn Sie daraufdrücken, erscheint ein Fenster, in dem Sie die zu installierende Datei auswählen können:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



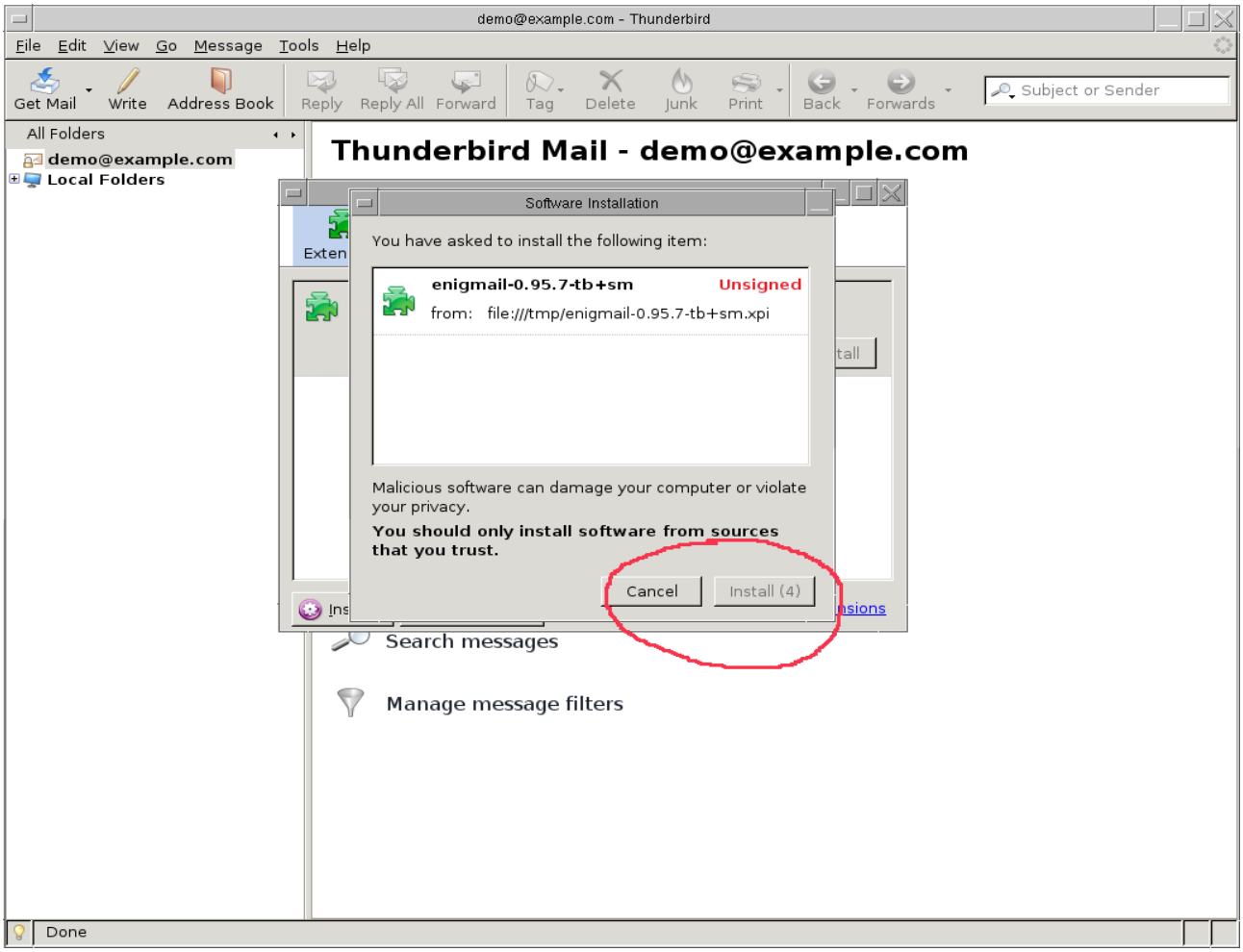
Nachdem Sie die Erweiterung auf Ihrer lokalen Festplatte gespeichert haben, gehen Sie wieder zurück zu dem Erweiterungsdialog in Thunderbird (siehe zweites Bild von oben) und drücken auf „Installieren...“:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Sie wählen die richtige Datei aus und folgen den Anweisungen. Um Ihnen Zeit zu geben, Ihre Entscheidung noch einmal zu überdenken, fügt Thunderbird automatisch eine kleine Wartezeit ein. Wenn die Zeit abgelaufen ist, ändert sich die Beschriftung des Knopfes, und Sie können mit der Installation fortfahren. Das wird auf den beiden folgenden Bildern gezeigt.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

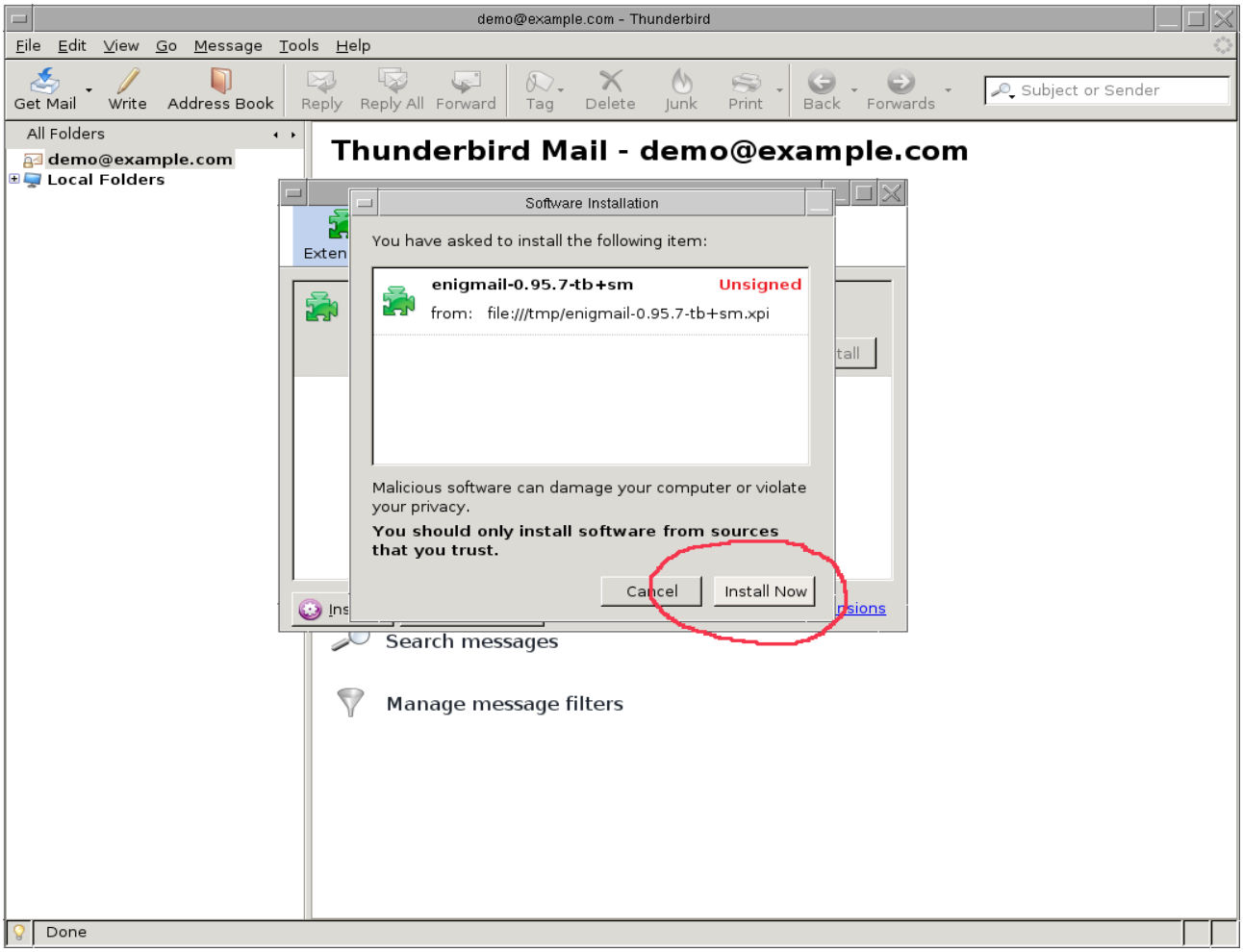


Zum Hochwald 20
D-51674 Wiehl
Tel. +49 2261 979364

http://www.oeko.net
AS29394

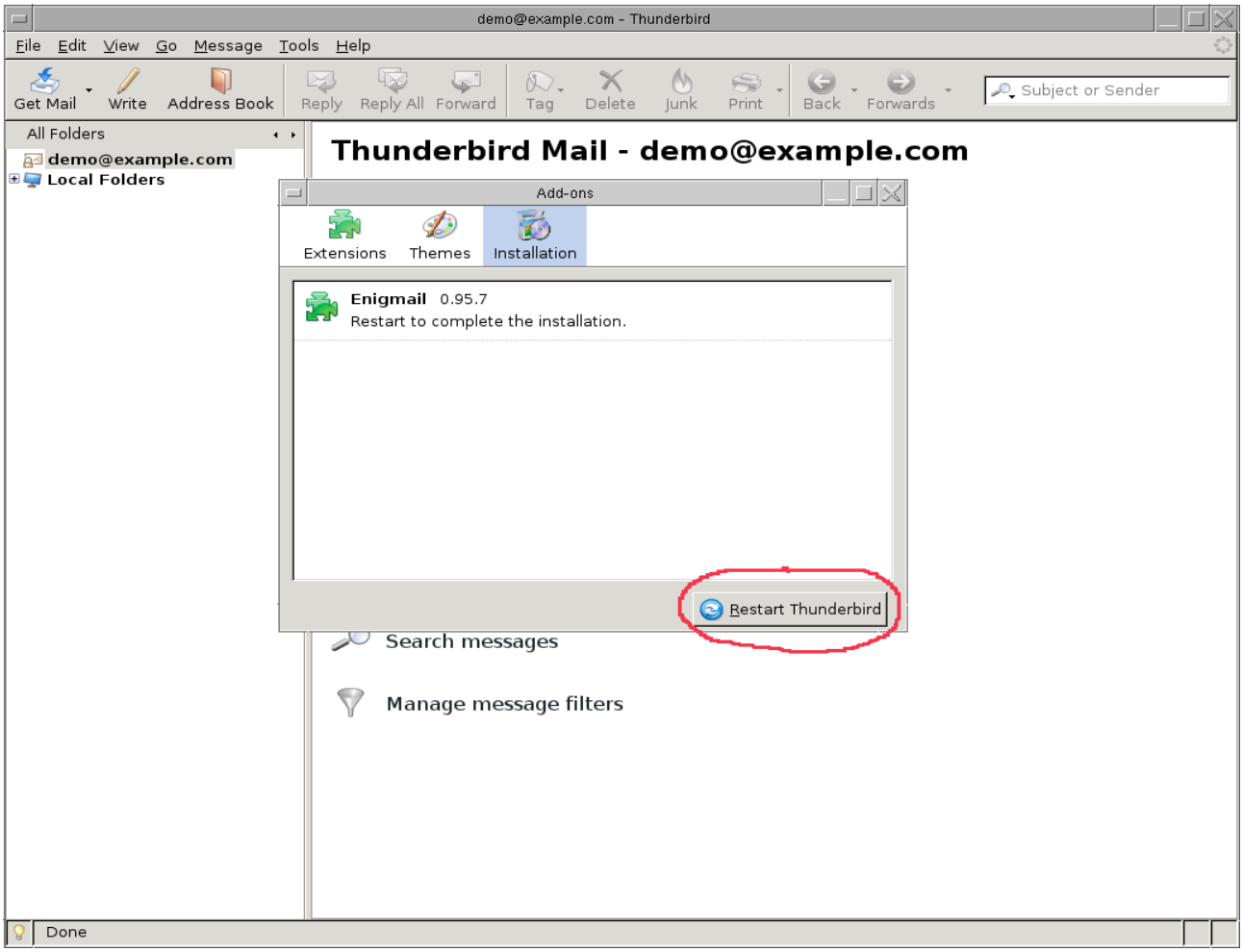
Inhaber: Dip..-Inf. Toni Müller
Dipl.-Ing. Imke Brandt

gegründet 1993
online seit 1994



Nach dem Abschluß der Installation müssen Sie Thunderbird neu starten, damit die Erweiterung aktiviert werden kann:

Zum Hochwald 20
D-51674 Wiehl
Tel. +49 2261 979364
http://www.oeko.net
AS29394
Inhaber: Dip..-Inf. Toni Müller
Dipl.-Ing. Imke Brandt
gegründet 1993
online seit 1994



Zum Hochwald 20
D-51674 Wiehl
Tel. +49 2261 979364

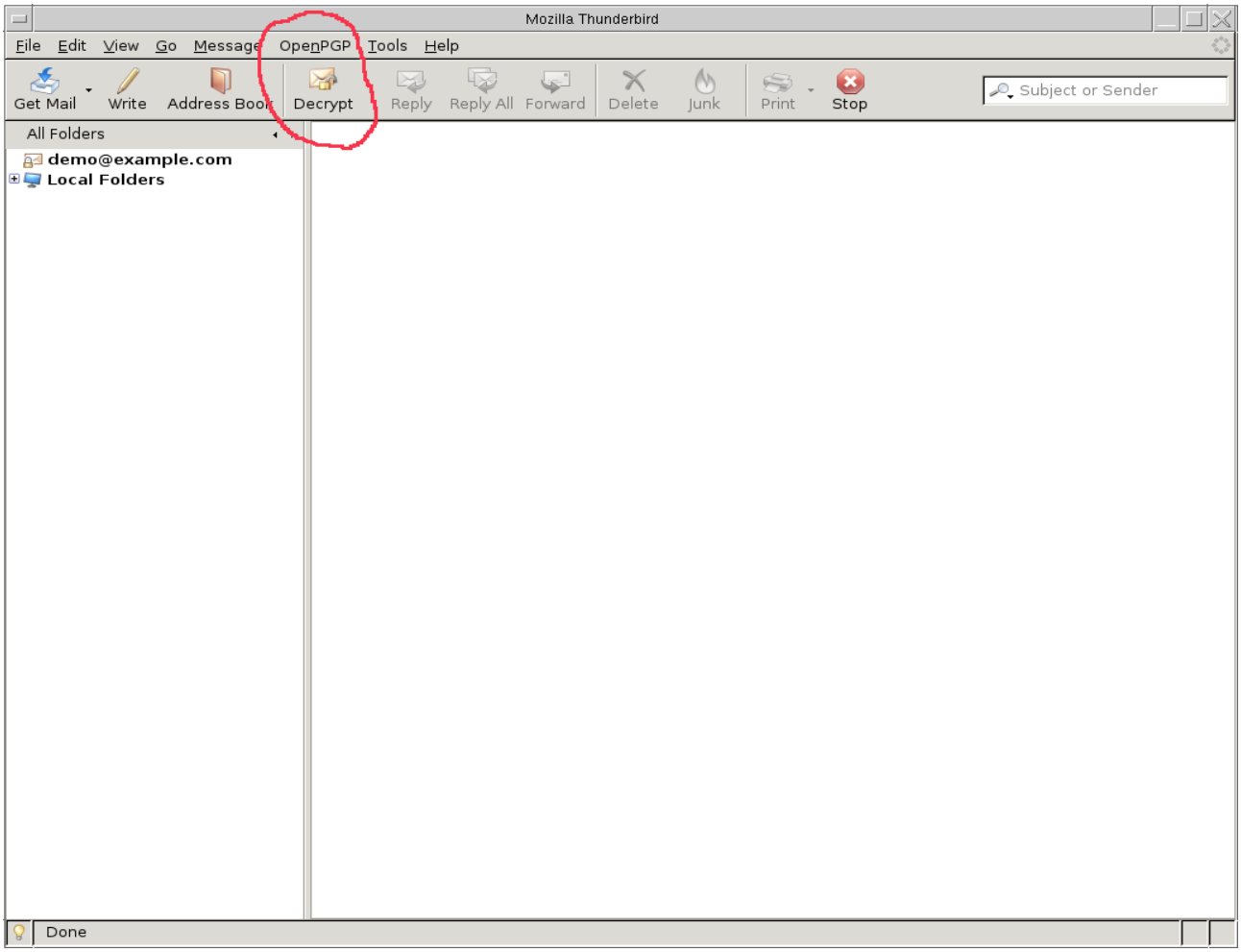
http://www.oeko.net
AS29394

Inhaber:
Dip..-Inf. Toni Müller
Dipl.-Ing. Imke Brandt

gegründet 1993
online seit 1994

Einrichtung von GnuPG und Enigmail

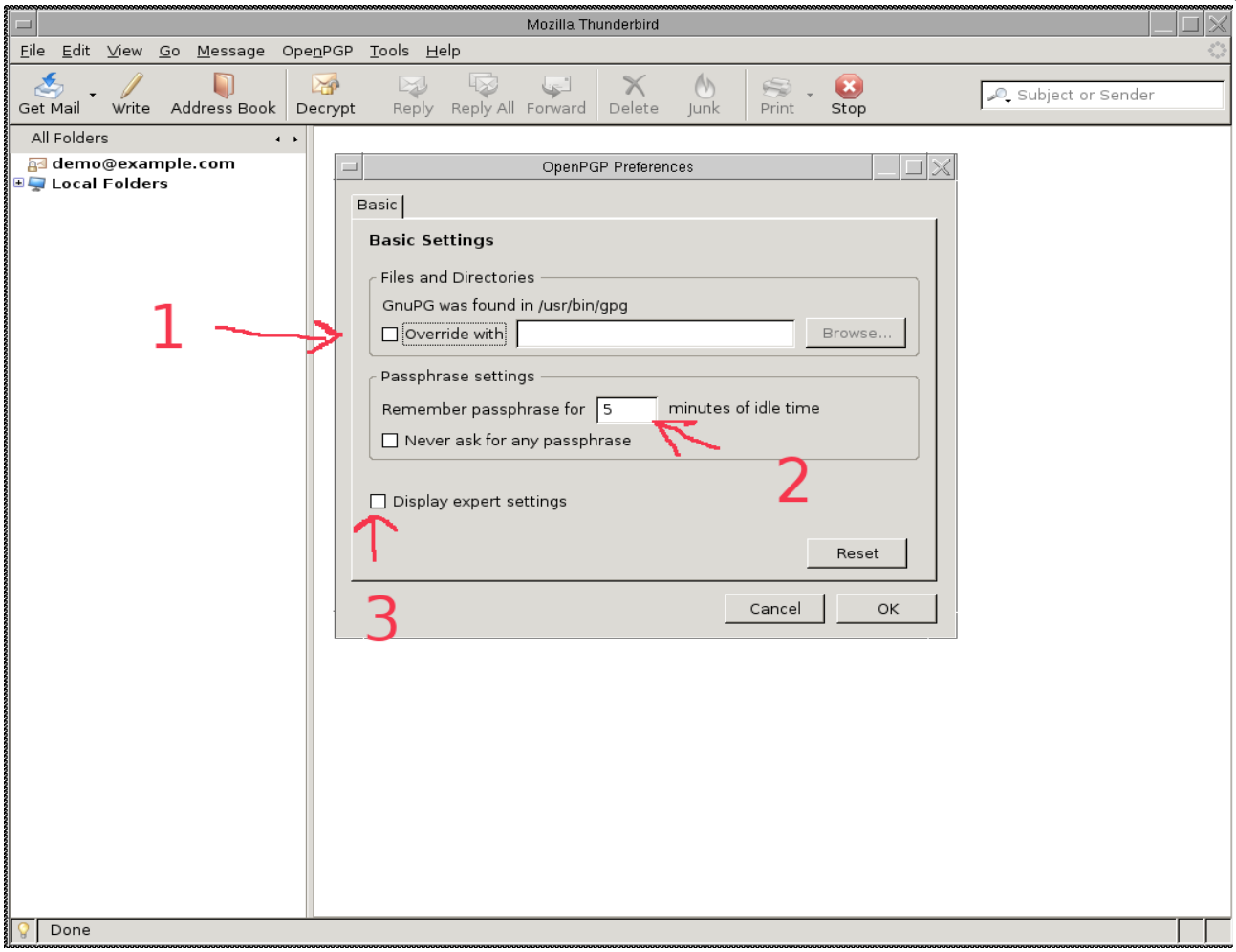
Nach dem Neustart von Thunderbird finden Sie auf der Oberfläche zwei neue Bedienelemente, die mit Emailverschlüsselung zu tun haben:



Zunächst muß die Software konfiguriert werden. Zum Beispiel müssen erst Schlüssel zur Verfügung stehen, bevor man etwas verschlüsseln kann, und bevor Sie eine Datei signieren können, benötigen Sie ein Schlüsselpaar, wie oben beschrieben.

Wir beschreiben als Nächstes die Grundeinstellungen der Software und die Erzeugung eines Schlüsselpaares:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



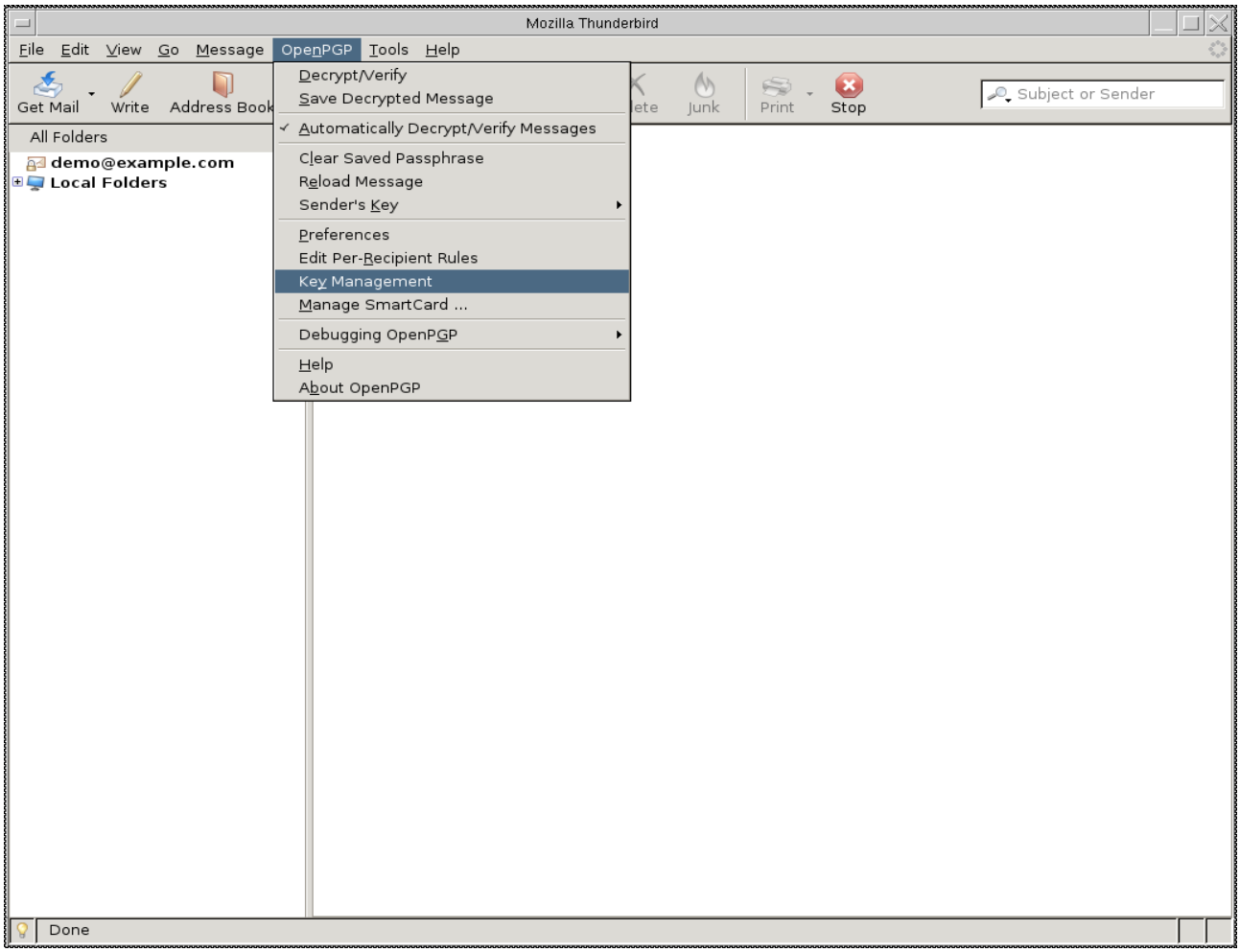
1. Falls das „gpg“-Programm (Teil des GnuPG-Paketes, jedenfalls unter Linux), das die eigentlichen Verschlüsselungsaufgaben erledigt, nicht gefunden werden kann, können Sie hier den korrekten Pfad zu dem Programm eintragen. Das könnte erforderlich sein, wenn Sie das Programm an einer ungewöhnlichen Stelle installiert haben. Unter Windows könnte das Programm etwa unter C:\Programme\GnuPG\gpg.exe oder an einem ähnlichen Ort und einem ähnlichen Namen zu finden sein.
2. In dem Feld „Passphrase-Einstellungen“ kann man einstellen, wie lange die Passphrase[1] halten soll. Hier kann man einen Mittelwert zwischen Bequemlichkeit und Sicherheit wählen, allerdings sollte man das Feld „Nie nach der Passphrase fragen“ **NIE** ankreuzen, da dies eine massive Sicherheitslücke öffnen dürfte.
3. Zu guter Letzt kreuzen wir „Experteneinstellungen anzeigen“ an.

1 Die „Passphrase“ ist eine Art sehr langes Paßwort. Wir gehen später noch darauf ein.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

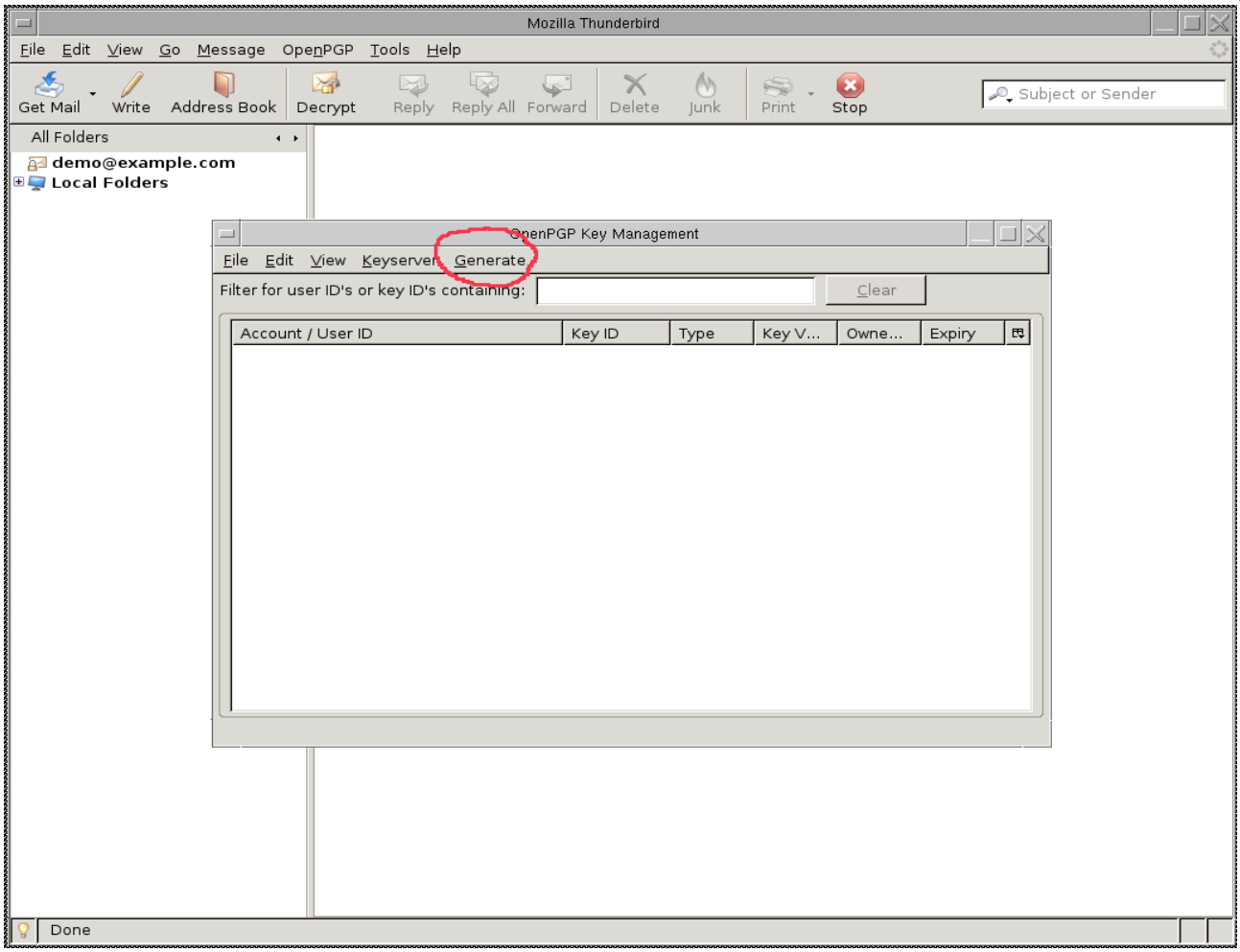
Erzeugung eines Schlüsselpaares

Als nächsten Schritt erzeugen wir uns ein Schlüsselpaar, ohne das wir von unserer Emailverschlüsselung keinen Gebrauch machen können:

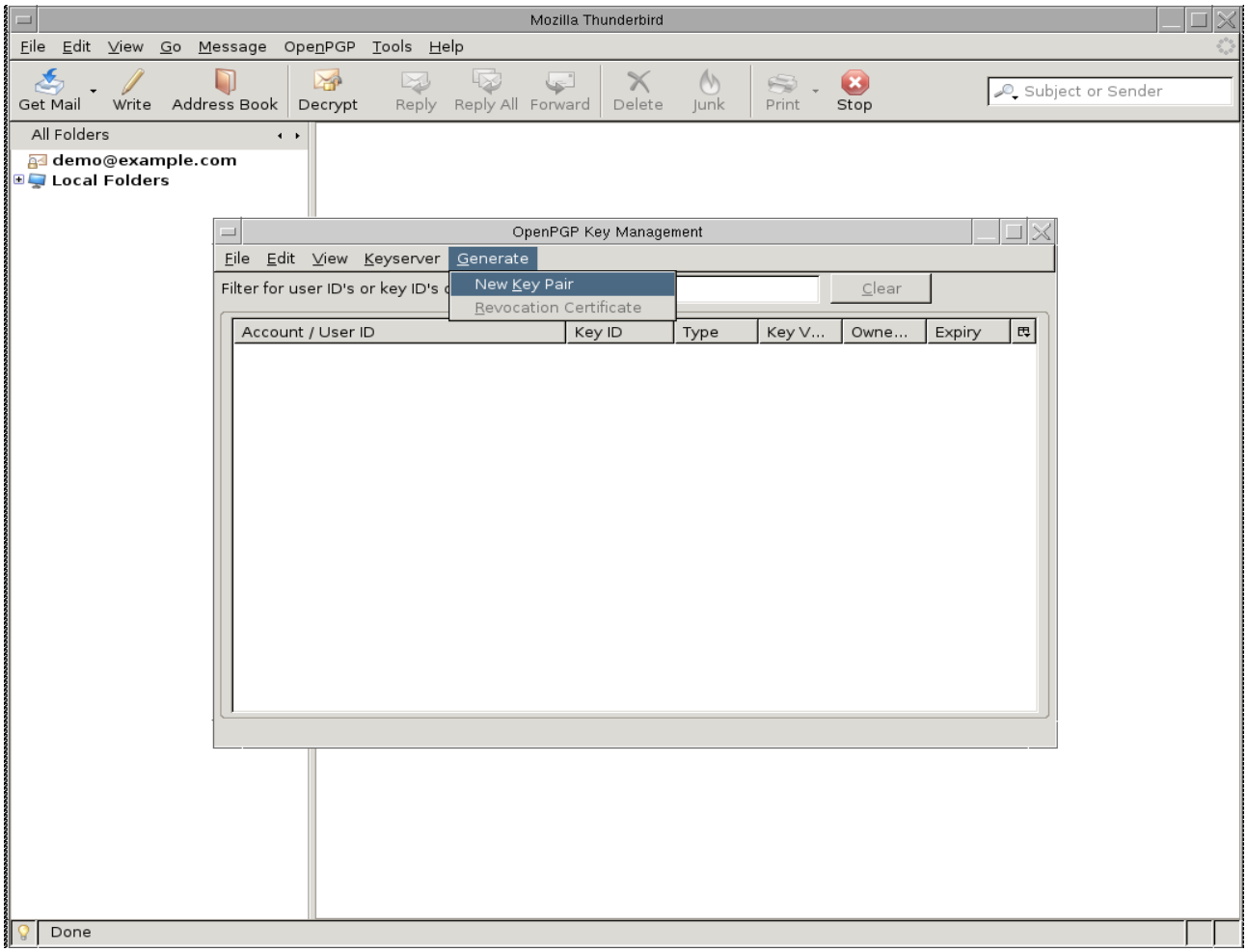


Wenn Sie vorher noch nie mit Verschlüsselung gearbeitet haben, dann zeigt Ihnen das System nun in der Liste der Schlüssel keine Schlüssel an. Wir wählen einfach den Menuepunkt „Schlüssel erzeugen“:

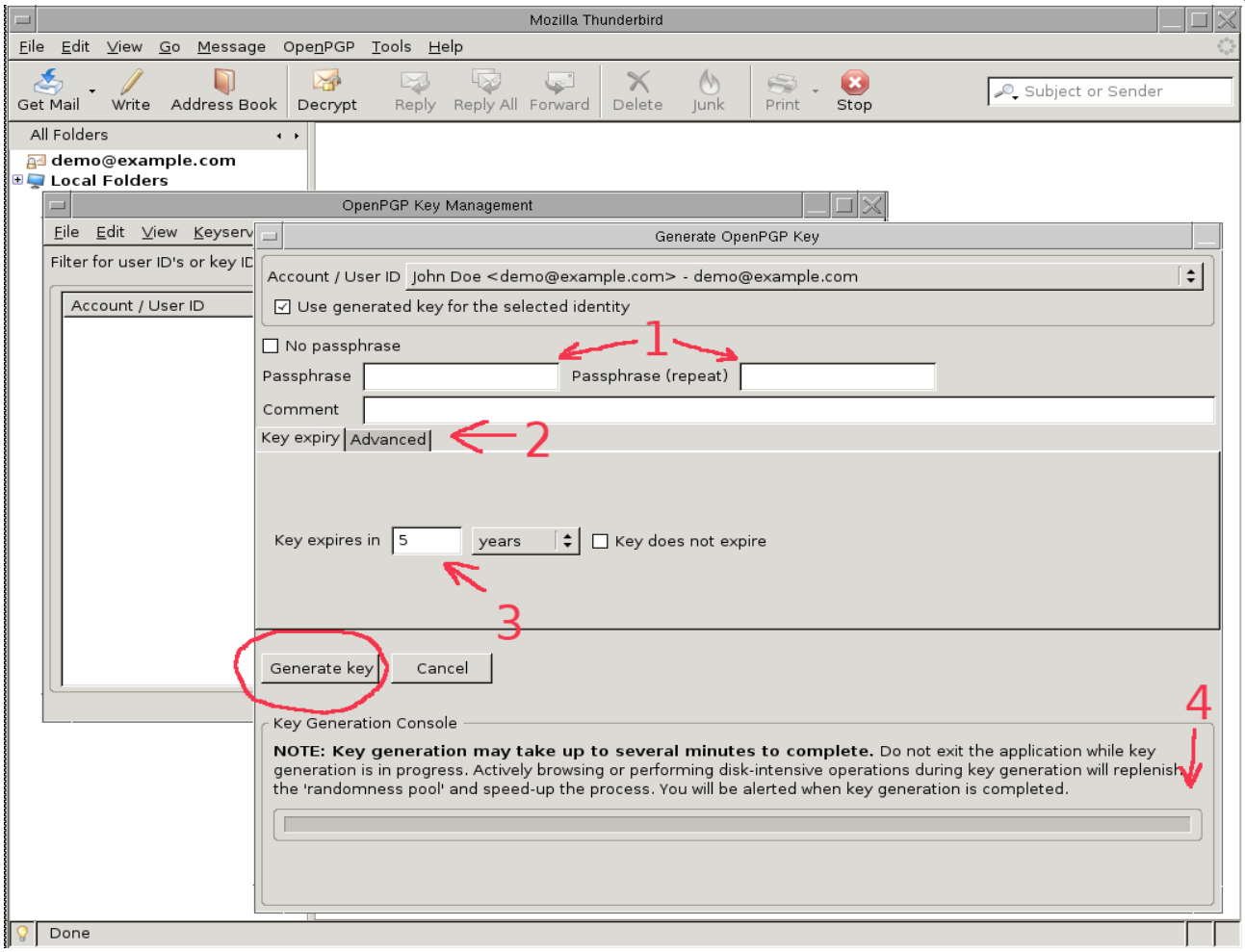
Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



In dem folgenden Dialog gibt es etliche Einstellmöglichkeiten, die weiter unten erklärt werden. Es ist aber nur halb so schlimm, wie es auf den ersten Blick aussieht:



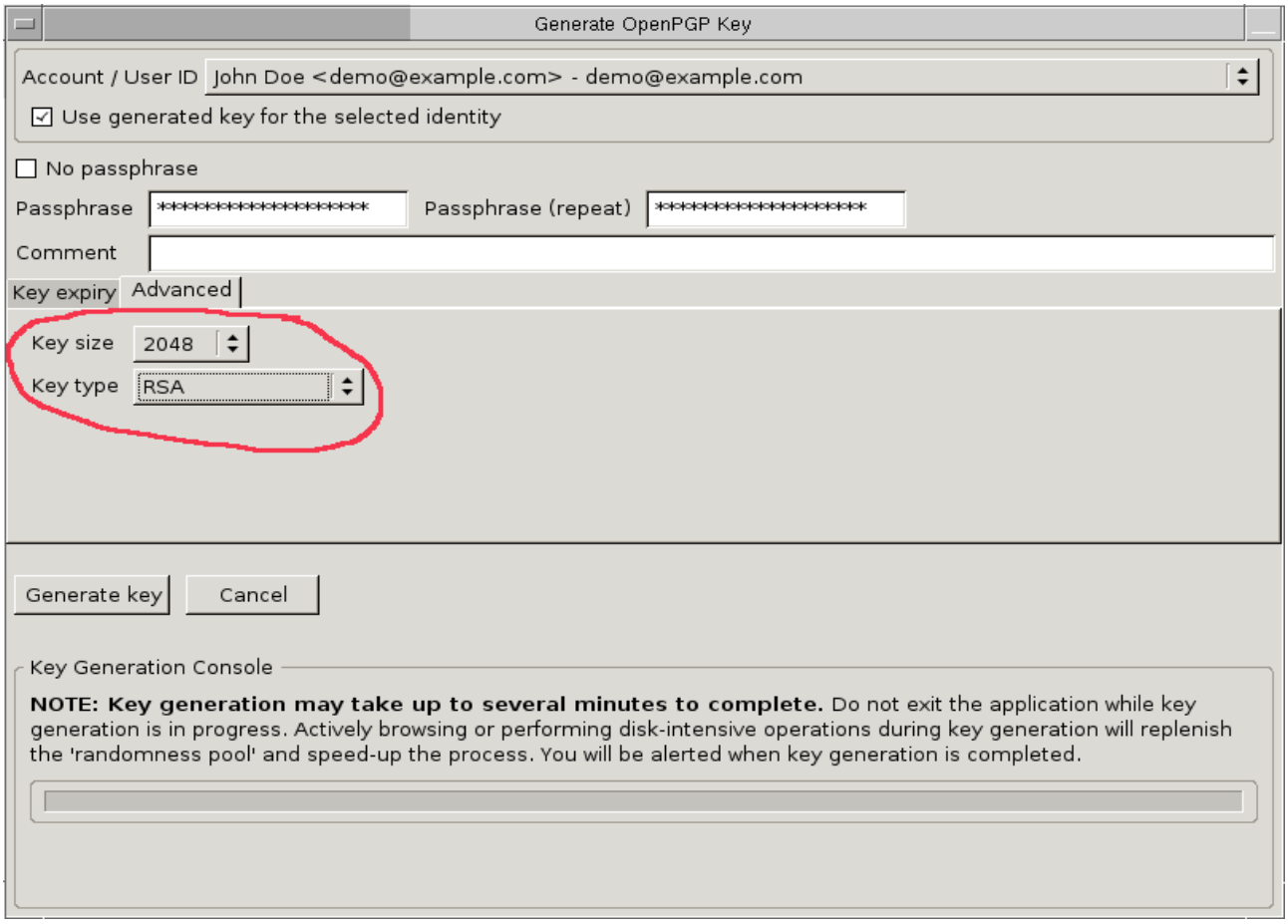
1. Sie werden zur zweimaligen Eingabe einer sogenannten „Passphrase“ aufgefordert. Bei der Passphrase handelt es sich quasi um ein Paßwort (Kennwort, Parole, ...), mit der Ihr privater Schlüssel gegen Mißbrauch gesichert wird. Sie müssen bei jeder Verwendung des privaten Schlüssels, also zum Entschlüsseln oder Signieren einer Nachricht, diese Passphrase eingeben. Das Programm kann sich, wie weiter oben dargestellt, die Passphrase für eine gewisse Zeit merken, so daß Sie, wenn Sie viele Verschlüsselungsoperationen ausführen wollen, nur ab und zu die Passphrase eingeben müssen. Aber da die Sicherheit des Gesamtsystems wesentlich von der kryptograpischen Stärke dieser Passphrase abhängt, also salopp ausgedrückt davon, wie schwer die Passphrase zu raten ist, sollte man sich hier eine wirklich gute Passphrase ausdenken. **Empfohlen sind Zeichenketten aus Buchstaben, Ziffern und Sonderzeichen mit einer Länge von mindestens 20, besser 30, Zeichen. Wenn Sie die Passphrase verlieren, verlieren Sie gleichzeitig den Zugang zu Ihren verschlüsselten Emails. Wenn jemand die Passphrase rät und z.B. Ihren Computer klaut, kann er sich als Sie ausgeben (Identitätsdiebstahl).**

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

2. Der Reiter „Advanced“ („Erweitert“, ...) bietet Ihnen die Möglichkeit, bestimmte Eigenschaften Ihres Schlüssels festzulegen, vor allem die Schlüssellänge, sowie das genaue Verfahren, nachdem die Verschlüsselung arbeiten soll. Die derzeit voreingestellten Standardwerte sind 2048 Bit für die Schlüssellänge und DSA/ElGamal für das Verschlüsselungsverfahren. Seit einiger Zeit jedoch gibt es eine Diskussion darüber, statt DSA/ElGamal auf RSA-Verschlüsselung zu setzen. Falls Sie hohes Zutrauen zu Ihren Fähigkeiten, Ihren Computer frei von Schadsoftware und unerwünschtem Zugriff zu halten, empfiehlt es sich, die Schlüssellänge auf 4096 Bit umzustellen. Die Schlüssellänge kann ganz grob als Maßstab dafür angesehen werden, wie schwer es ist, Ihre Verschlüsselung zu knacken, wenn man den privaten Schlüssel nicht besitzt. 1024 Bit sind heutzutage schon als ziemlich knapp anzusehen, und die Fortschritte in der Kryptographie, also dem Zweig der Mathematik, der sich mit Verschlüsselung befaßt, sowie in der Computertechnik, lassen nach und nach immer längere Schlüssel in die „Reichweite“ von Angreifern gelangen. Ein Schlüssel von 2048 Bit Länge sollte allerdings noch einige Jahre als „sicher“ gelten.
3. Um dem Problem, daß Schlüssel durch die Fortschritte in Wissenschaft und Technik im Laufe der Zeit automatisch schwächer werden, zu begegnen, versieht man Schlüssel heute mit einem Verfallsdatum. Der voreingestellte Wert, fünf Jahre, bedeutet, daß Ihr Schlüssel in fünf Jahren automatisch ungültig wird, so daß danach keine Email mehr mit diesem Schlüssel verschlüsselt, und, was in der Praxis noch viel wichtiger ist, signiert werden kann.
4. Wenn Sie auf „Schlüssel erzeugen“ („Generate key“) drücken, wird unten ein Fortschrittsbalken zu der Erzeugung des Schlüssels, was erhebliche Zeit in Anspruch nehmen kann, angezeigt. Der Vorgang darf nicht unterbrochen werden.

Hier noch zwei Abbildungen zu den erweiterten Einstellungen:

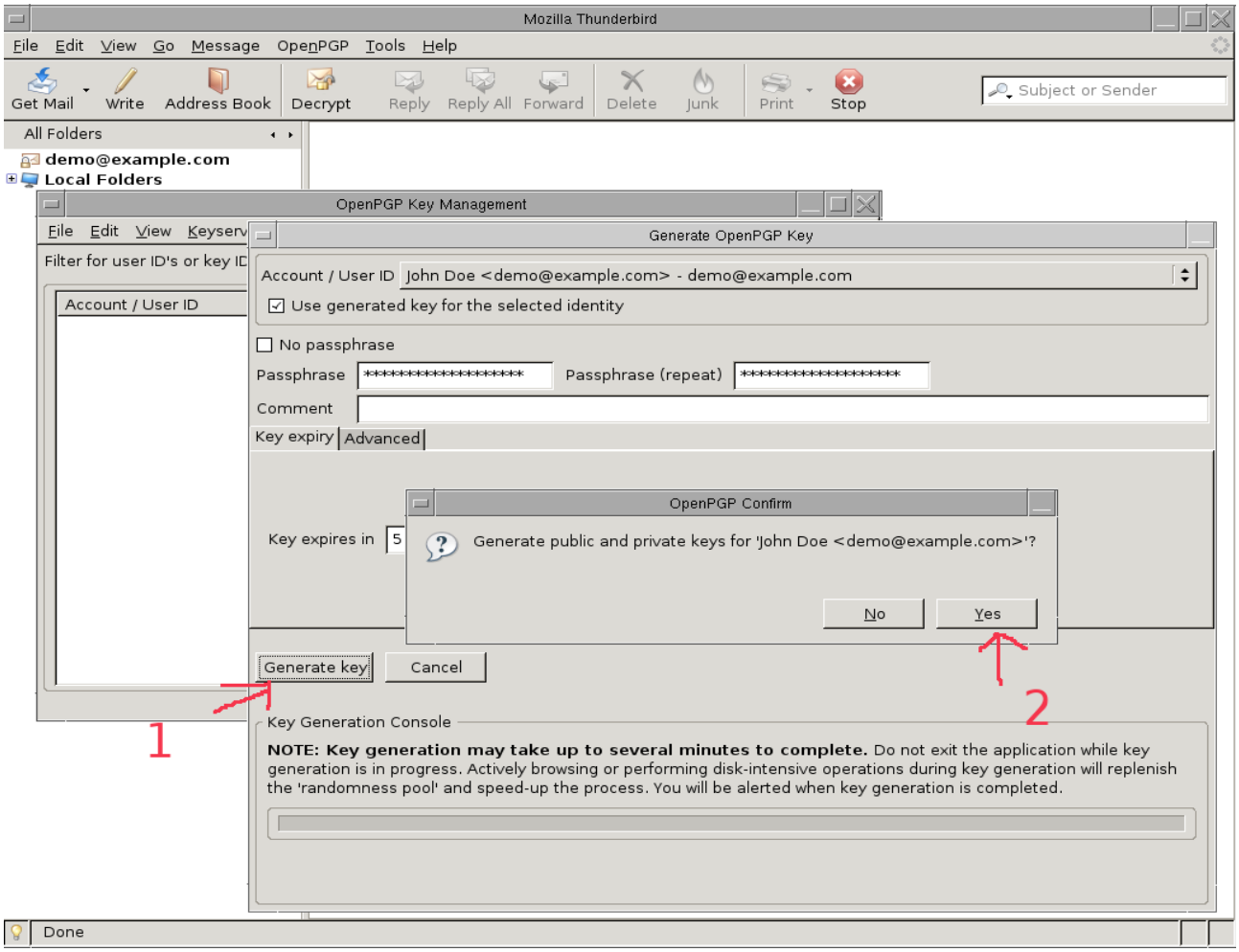
Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Wenn Sie bereit sind, den Schlüssel zu erzeugen, drücken Sie auf den Knopf. Sie müssen dies noch einmal bestätigen. Für die Erzeugung des Schlüssels ist es von großer Bedeutung, gute Zufallszahlen zu haben. Computer erzeugen diese Zufallszahlen normalerweise aus ihren Betriebsparametern, bevorzugt mittels der Festplattenaktivität. Wenn Ihnen die Zeit lang wird, empfiehlt es sich, zwischendurch Dinge mit dem Computer anzustellen, die viel Festplattenaktivität verursachen, etwa viele Dateien durchsuchen zu lassen, oder viele Dateien hin- und herzukopieren.

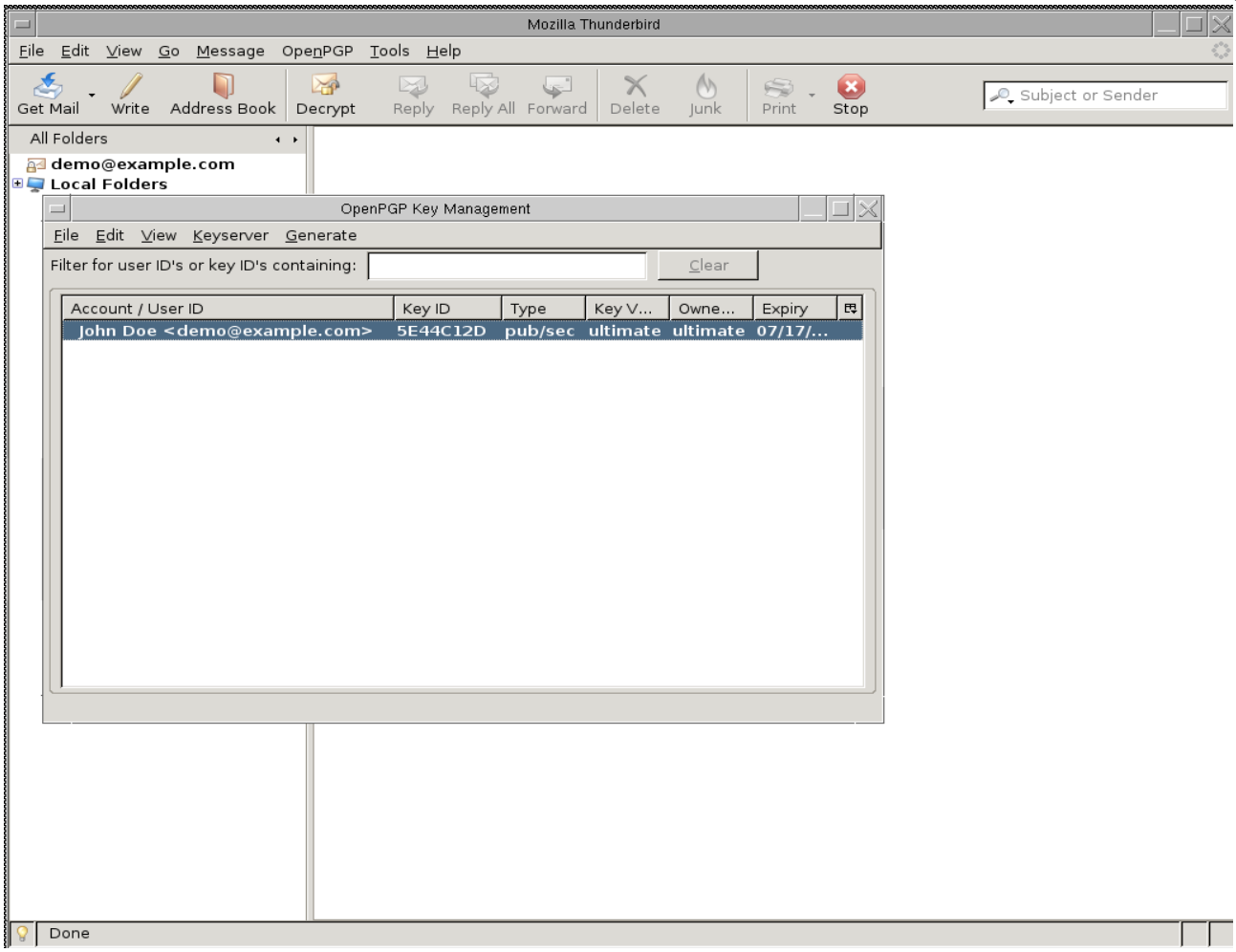
Die Abfolge in der Bedienung wird im folgenden Bild dargestellt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Wenn das Schlüsselpaar erzeugt wurde, wird es in dem Dialog zur Schlüsselverwaltung angezeigt:

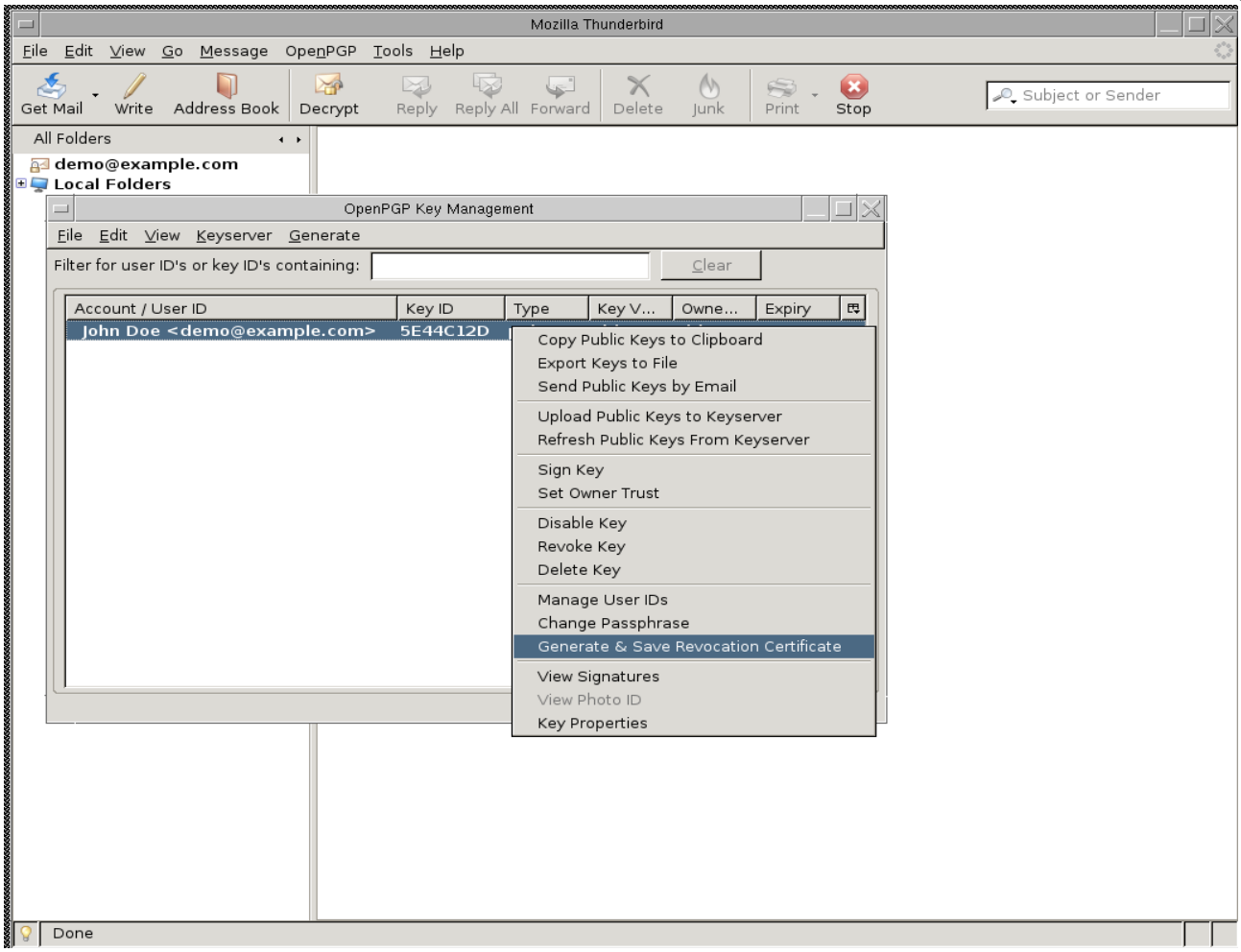
Zum Hochwald 20
D-51674 Wiehl
Tel. +49 2261 979364
http://www.oeko.net
AS29394
Inhaber: Dip..-Inf. Toni Müller
Dipl.-Ing. Imke Brandt
gegründet 1993
online seit 1994



Vorher wird man noch zur Erzeugung eines sogenannten „Revocation Certificate“s aufgefordert. Dabei handelt es sich um eine spezielle Art von Schlüssel, mit der man einen Schlüssel schon vor dem Ablaufdatum für ungültig erklären kann. Wenn also Ihr öffentlicher Schlüssel auf einem Keyserver liegt, wo ihn jeder herunterladen kann, und Sie z.B. die Passphrase verloren haben oder festgestellt haben, daß jemand Ihren privaten Schlüssel gestohlen hat, dann laden Sie diesen Schlüssel ebenfalls auf den Keyserver hoch. Das bewirkt, daß dann in Kürze niemand mehr Ihren Schlüssel benutzen kann. Das dient dem Schutz vor Mißbrauch kompromittierter Schlüssel. Selbstredend sollten Sie den „Revocation Certificate“ ebenfalls sehr sorgfältig verwahren und vor unbefugtem Zugriff schützen.

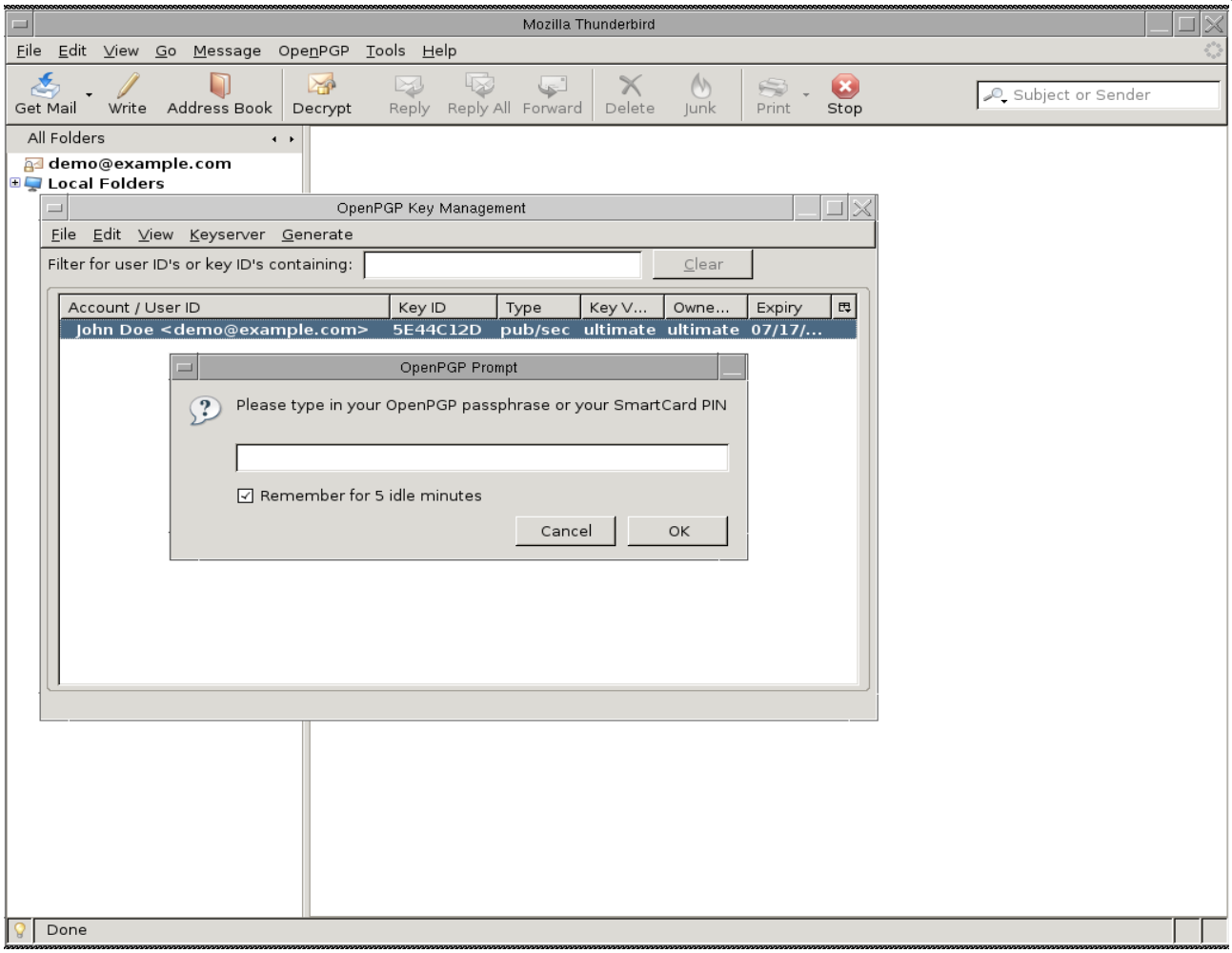
Diesen „Revocation Certificate“ („Rückhol-Zertifikat“) kann man jederzeit nachträglich erzeugen, indem man einen Schlüssel, zu dem man einen privaten Schlüssel besitzt (also einen **eigenen** Schlüssel), auswählt und diese Operation durchführt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



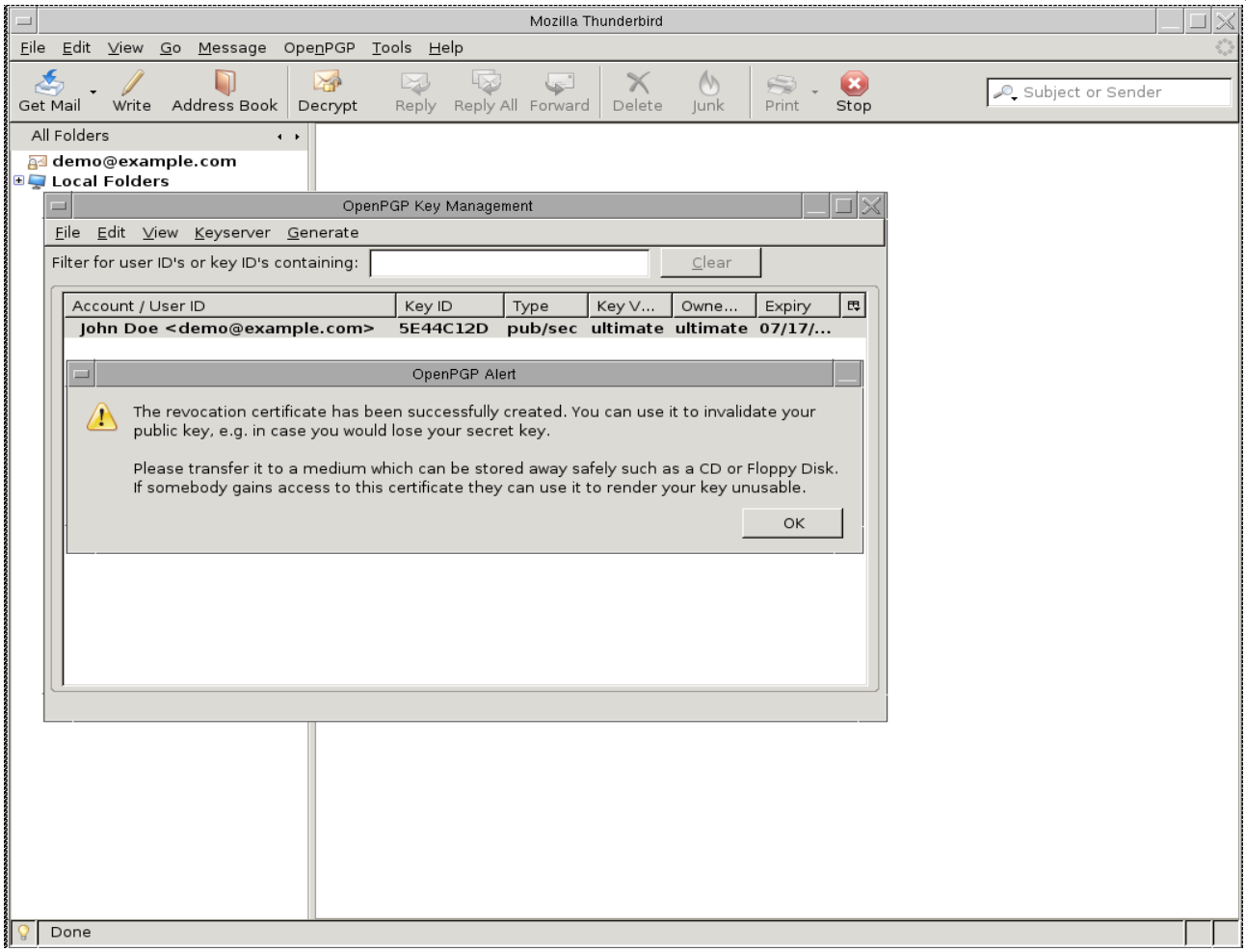
Sie werden aufgefordert, dieses Zertifikat irgendwo abzuspeichern. Bevor Sie allerdings dieses Zertifikat erzeugen können, müssen Sie sich durch die Eingabe der Passphrase als legitimer Besitzer des privaten Schlüssels ausweisen:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



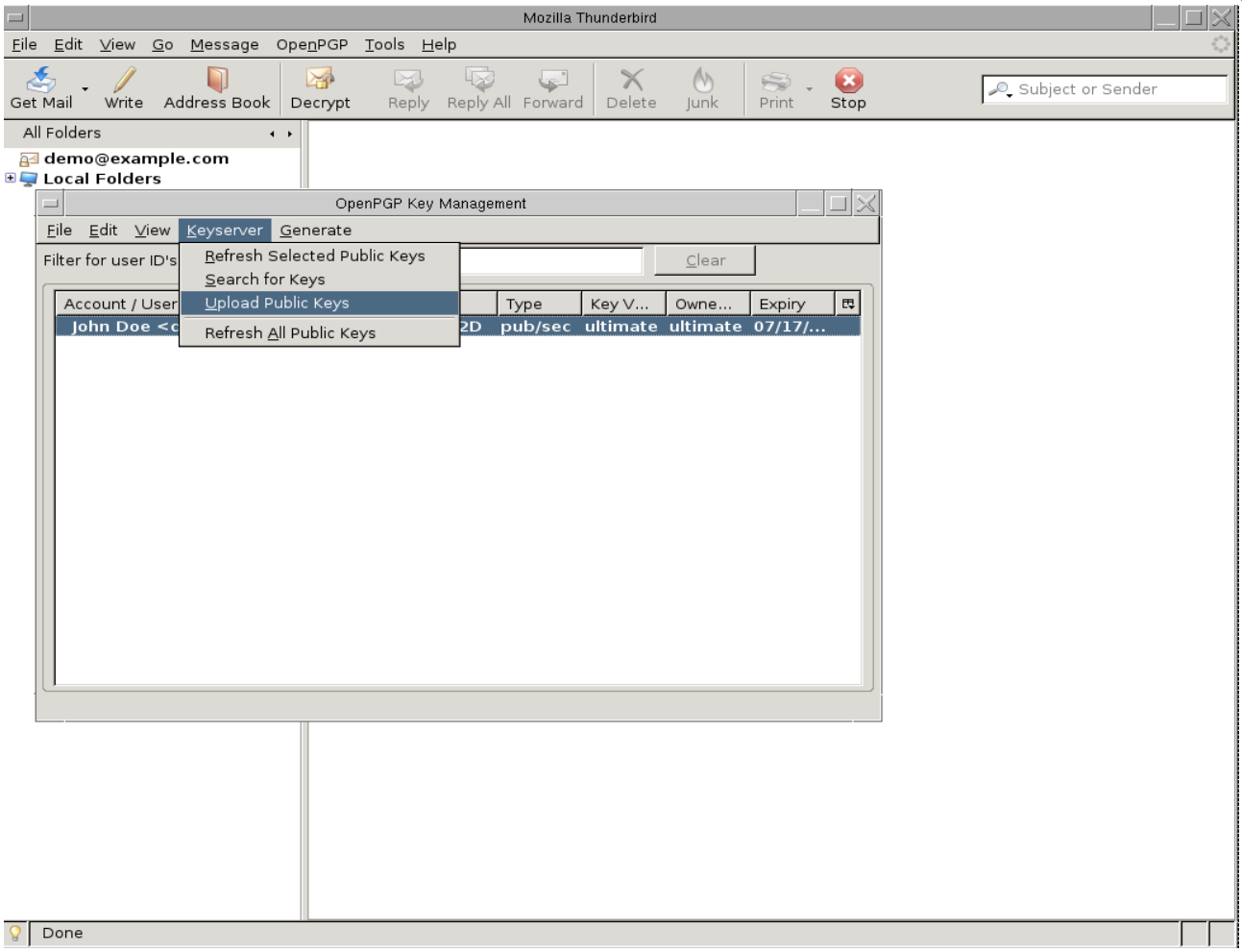
Sie geben die Passphrase ein und sehen noch folgenden Hinweis, der noch einmal auf die Bedeutung einer sicheren Verwahrung dieses Zertifikates hinweist:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

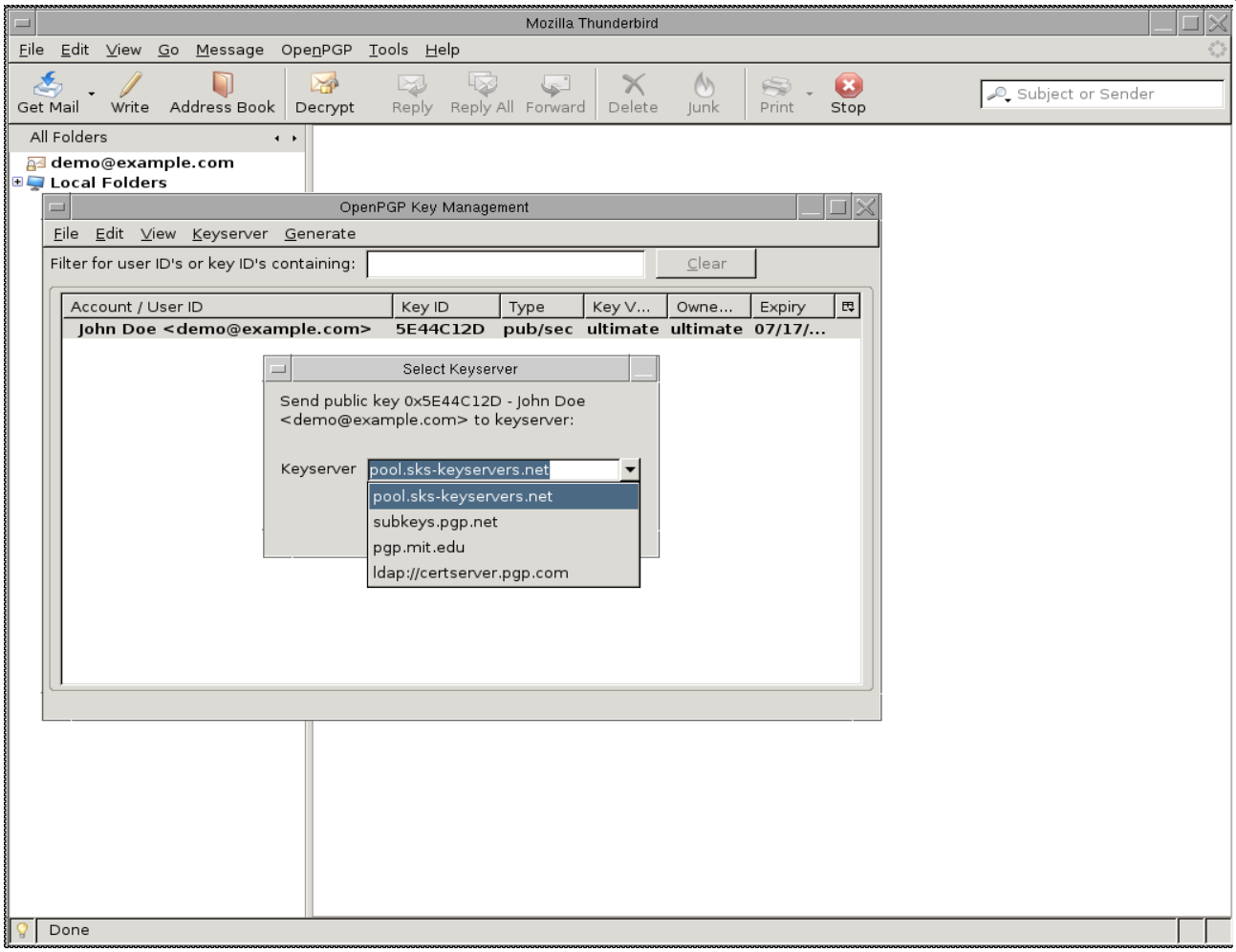


Der nächste Schritt ist in vielen Fällen das Hochladen des erzeugten (öffentlichen) Schlüssels auf einen Keyserver. Das hat für andere Nutzer den Vorteil, daß ihre Programme Ihren Schlüssel bei Bedarf automatisch herunterladen können, ohne irgendetwas eingeben zu müssen. Wenn Sie also beispielsweise eine digital signierte Email an einen anderen OpenPGP-Anwender verschicken und der einen Keyserver in seiner Konfiguration eingetragen hat, dann lädt sein Mailprogramm Ihren Schlüssel automatisch, oder mit nur einem Klick seitens des Anwenders, herunter. Dann kann der Anwender sofort sehen, ob die Signatur in Ordnung ist, oder Ihnen eine verschlüsselte Email zu schicken, ohne weitere Vorbereitungen treffen zu müssen:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Da die Keyserver unterschiedlich gut verfügbar, aber untereinander vernetzt sind, kann man den Schlüssel „irgendwohin“ hochladen. In Deutschland funktioniert unserer Ansicht nach dieser Keyserver besonders gut:

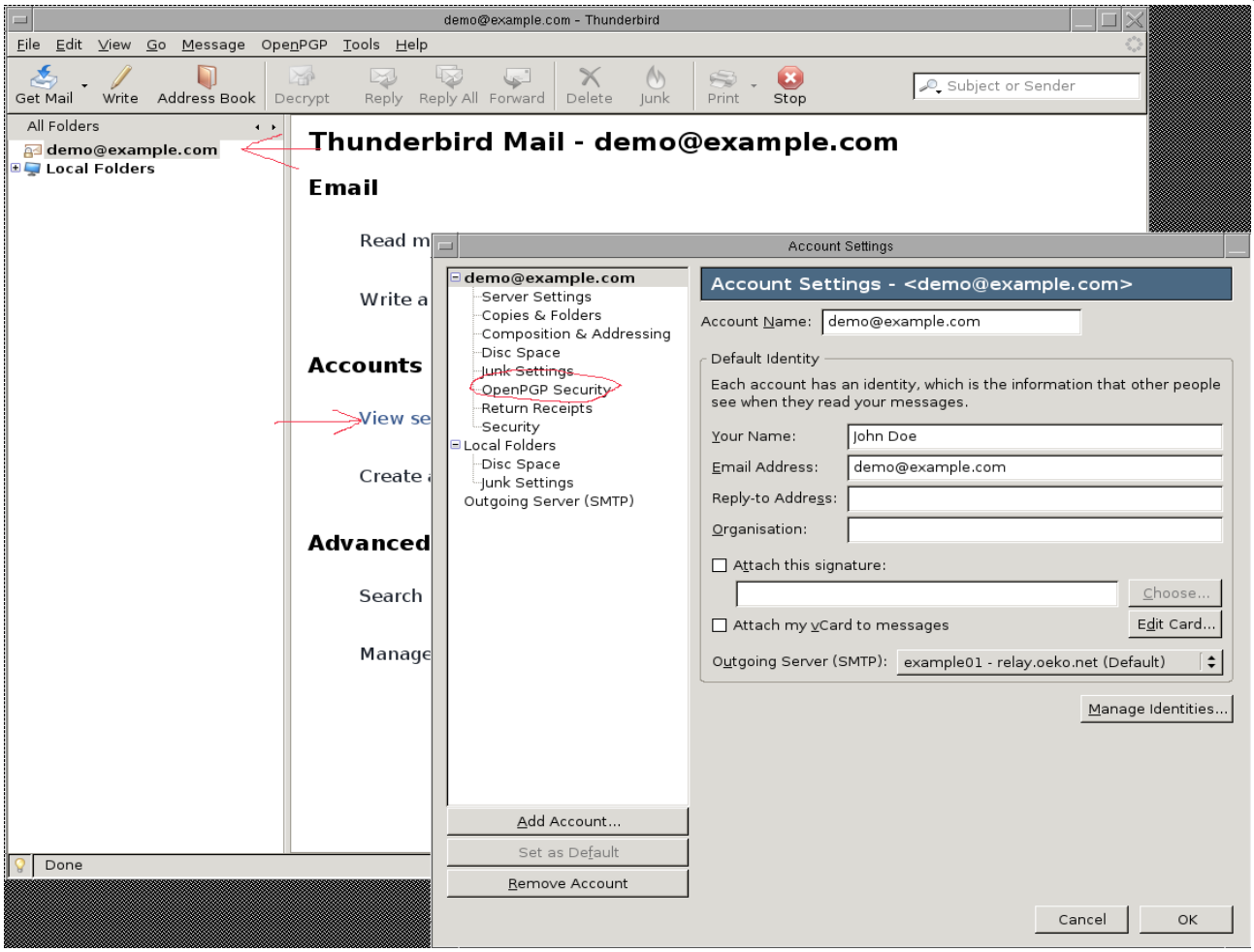
blackhole.pca.dfn.de

Da die Synchronisation der Keyserver untereinander mehrere Tage dauern kann, ist man mit einem lokalen, gut erreichbaren und gut gewarteten Keyserver unter Umständen besser als mit einem anderen, weiter entfernten, Keyserver bedient. Aber im Prinzip ist es egal, wo man seinen Key hochlädt.

Allgemeine Einstellungen

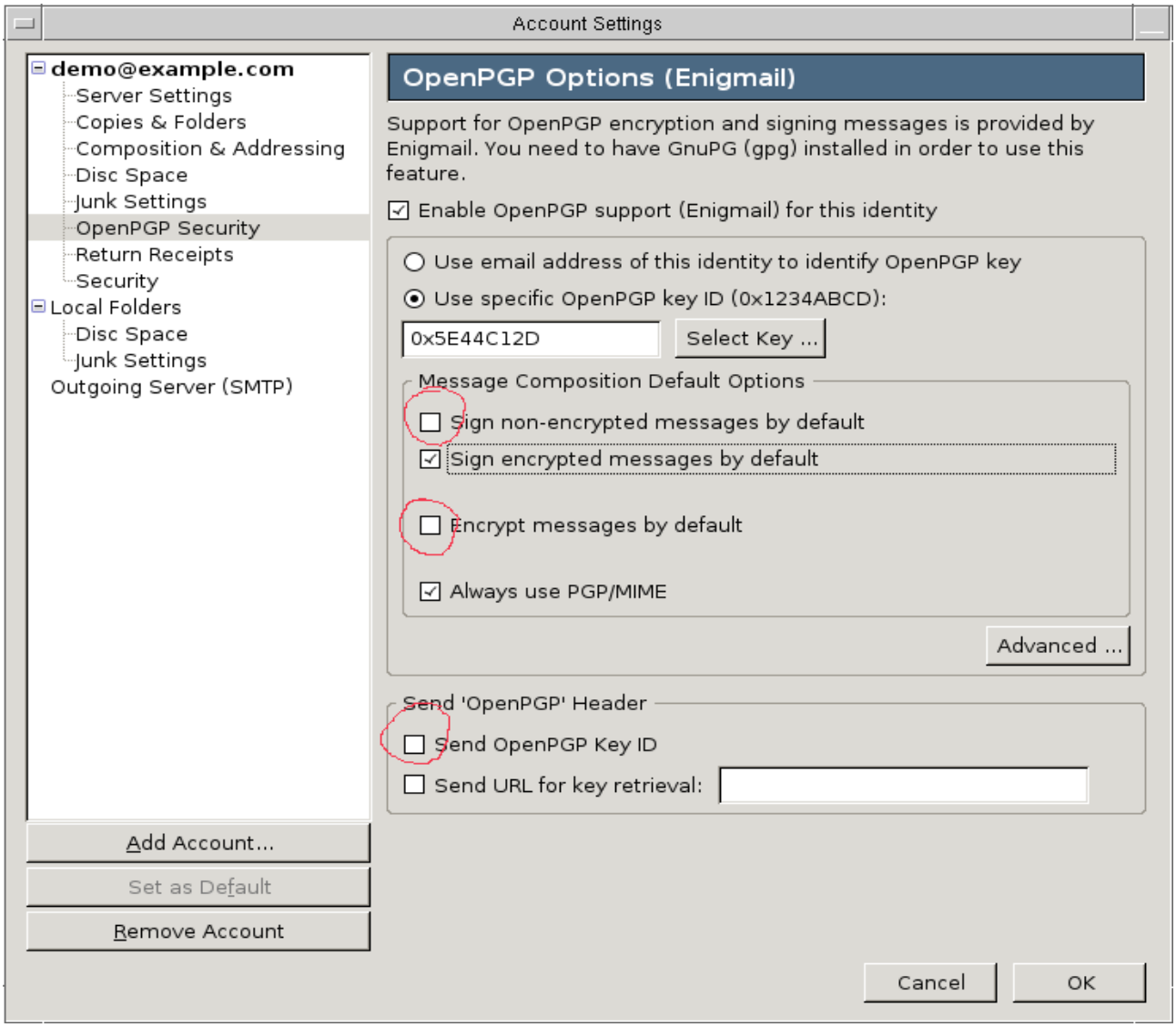
Außer den genannten Einstellungen sollte man noch einige andere Einstellungen vornehmen, die das Leben angenehmer machen. Dazu geht man auf die allgemeinen Kontoeinstellungen, wo sich ein neuer Menuepunkt findet:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Unter diesem Punkt wählt man „OpenPGP Security“ aus und kann dann die Einstellungen wie im nachfolgenden Bild empfohlen, vornehmen. Die eingekreisten Optionen kann man anschalten, die angekreuzten Punkte sollten auch angeschaltet sein:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



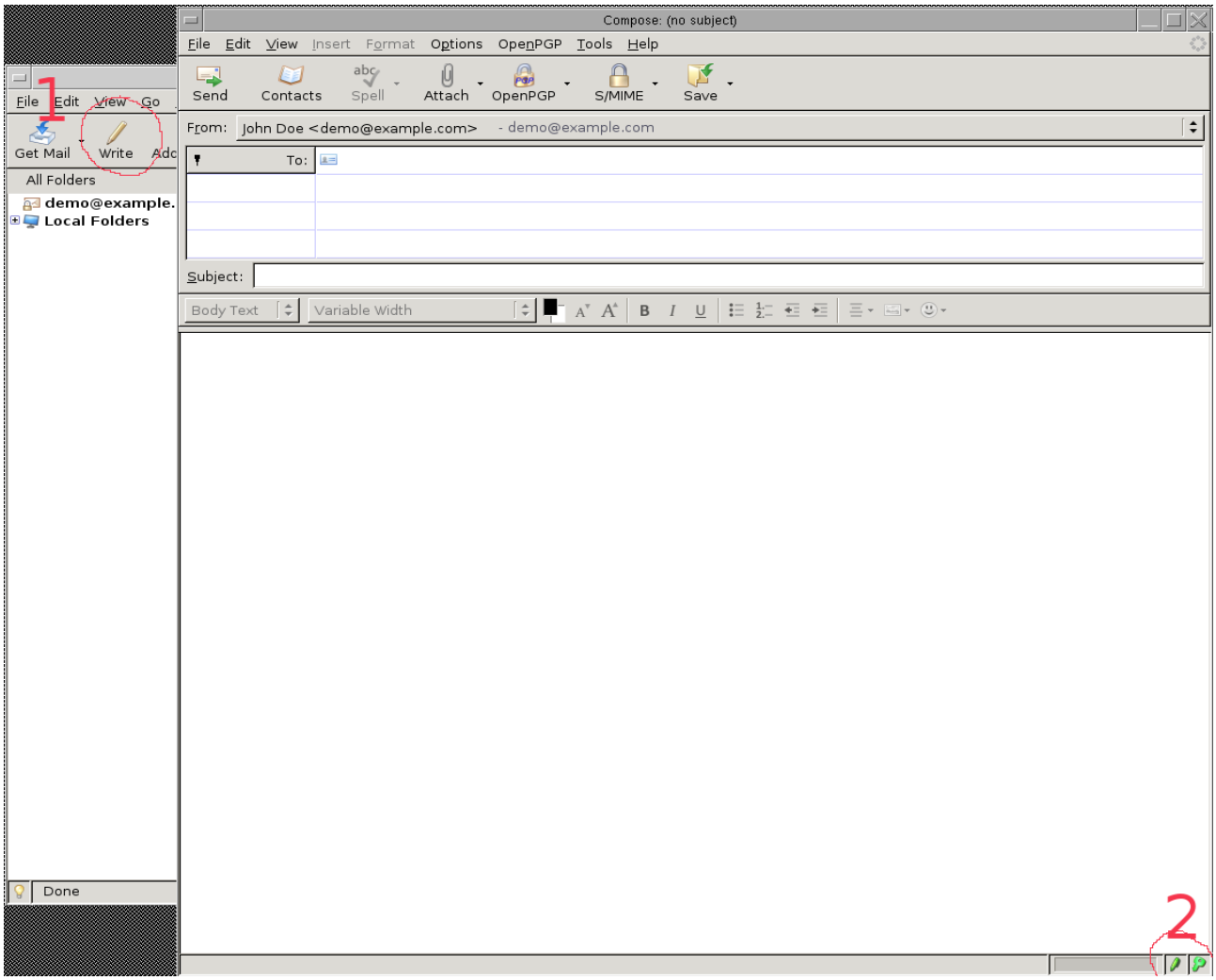
Zwar bewirkt der Punkt „Always use PGP/MIME“ für Benutzer von Outlook, daß diese Probleme beim Lesen der Email haben (es geht, ist aber umständlich in der Handhabung), aber für alle anderen Benutzer ist es eine Zumutung und ein Verlust an Funktionalität, wenn dieser Punkt nicht angekreuzt ist. Man kann hinterher pro Benutzer im Adreßbuch beziehungsweise in dem Menue mit den erweitern Optionen einstellen, daß die Mails für einzelne Benutzer nach dem PGP/MIME-Standard oder nach dem anderen Verfahren („Flowed“) verschlüsselt werden sollen. Da Outlook-Benutzer sowieso eine Menge Handarbeit erledigen müssen, wenn sie mit OpenPGP arbeiten, macht dieser Punkt den Kohl für Outlook-Benutzer auch kaum noch fett, aber immerhin werden damit nicht gleich alle Benutzer von ordentlichen Mailprogrammen bestraft.

Wenn man seine Mails signiert (erster eingekreister Punkt im obigen Menue), dann sagt man damit dem Empfänger: „Hier, das war wirklich ich“, und empfiehlt gleichzeitig das Verfahren. Außerdem geben manche Spamfilter Bonuspunkte für digital signierte Mails.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

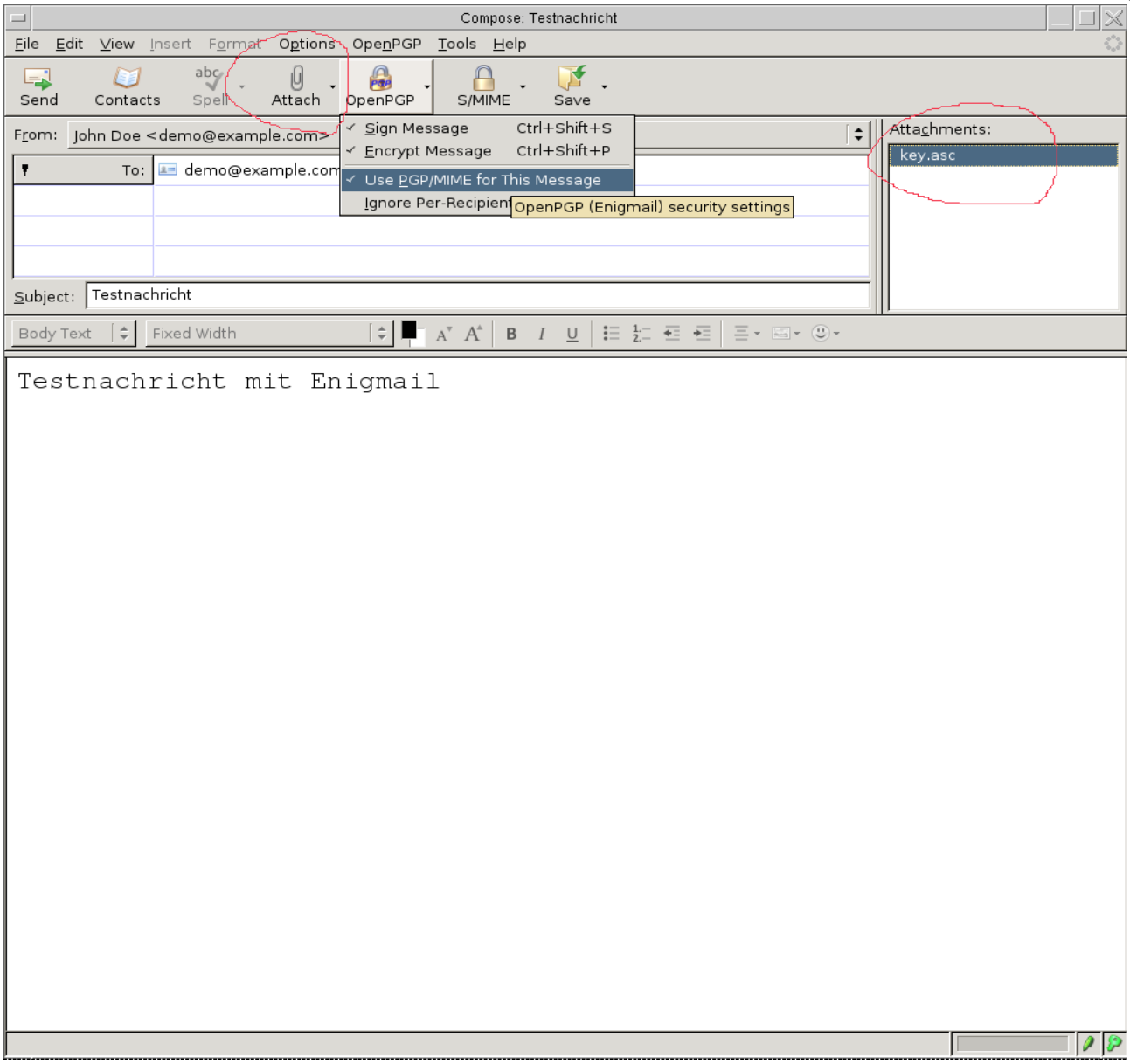
Versand von Emails

Nachdem das System nun konfiguriert ist, wollen wir zwei Beispiele im Detail durchspielen, einmal der Versand, und zum anderen der Empfang, von Emails. Zuerst versenden wir eine Email, der Einfachheit halber an uns selbst. Das folgende Bild zeigt den Knopf, auf den man zum Erstellen einer Email drückt, und die beiden Icons, mit denen man die beiden Funktionen „Verschlüsseln“ und „Signieren“ einfach einstellen kann. Natürlich sind dazu auch Menuepunkte am oberen Rand vorhanden.



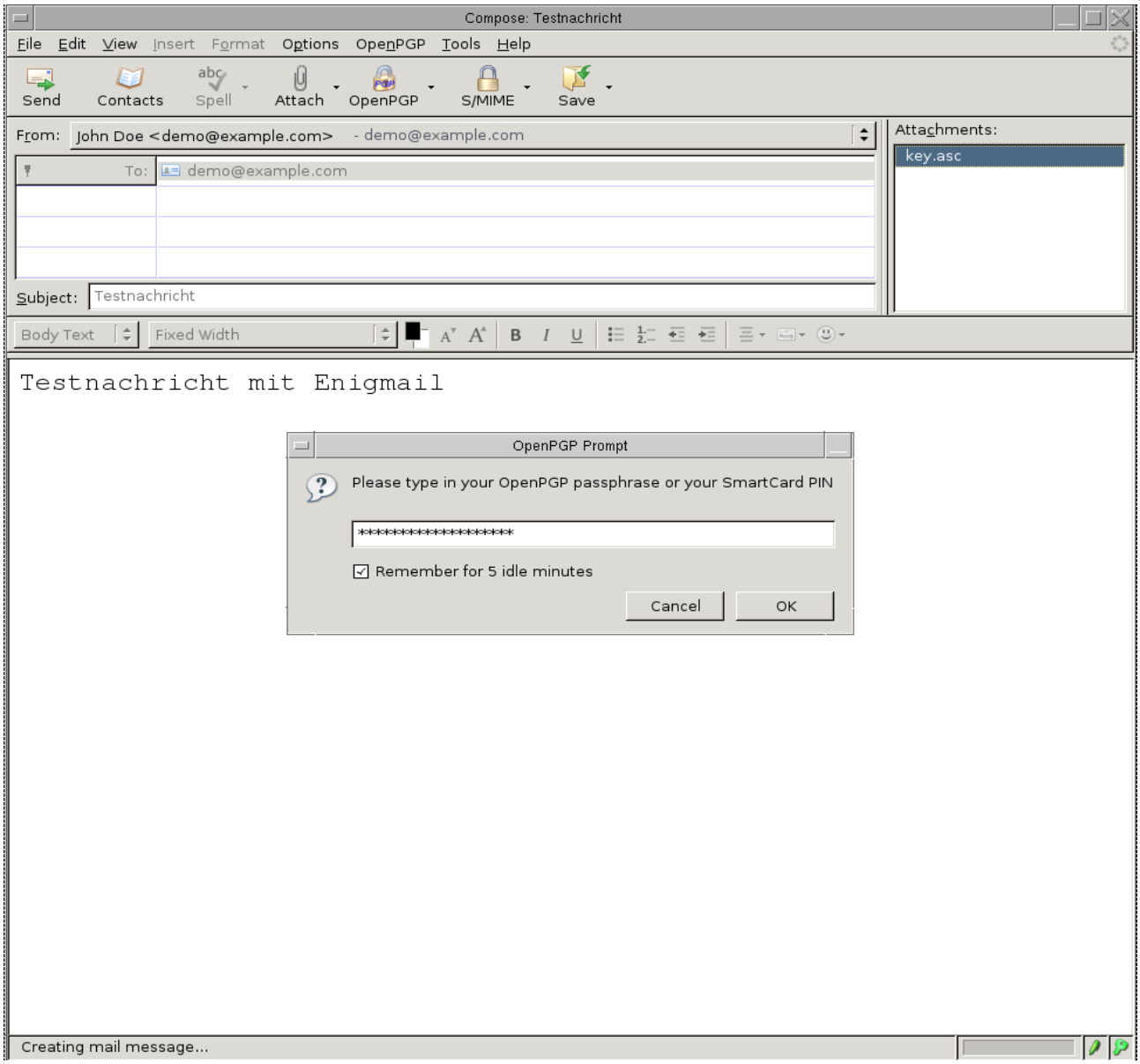
Sie können vor dem Versand der Nachricht noch einmal die Funktionen und das Nachrichtenformat einstellen. Die Beispielnachricht enthält einen Anhang. Der Versand von Anhängen, die mit verschlüsselt werden sollen, funktioniert **nur** mit der Option „PGP/MIME“, die wir ja als Standardverfahren eingestellt haben. In dem Bild sind der Knopf zum Öffnen des Anhangs-Dialogs und die Stelle, wo die Anhänge dargestellt werden, mit einem Kreis markiert. In dem aufgeklappten Menue ist der Punkt „PGP/MIME“ als Einstellung für das Nachrichtenformat markiert.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Wenn Sie die Nachricht versenden wollen, drücken Sie, wie gewohnt, auf den Knopf für „Senden“ (oben links mit dem grünen Pfeil nach rechts). Sie werden nun, da Sie „Signieren“ angekreuzt haben, nach der Passphrase zur Entsicherung des privaten Schlüssels gefragt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Wäre die Nachricht an jemand anders gegangen, hätten Sie gegebenenfalls noch einen Schlüssel auswählen und/oder herunterladen müssen. Allerdings kann Thunderbird in der Regel anhand der Emailadresse erkennen, welchen Schlüssel man nehmen sollte, so daß dieser Teil meist keine Arbeit macht.

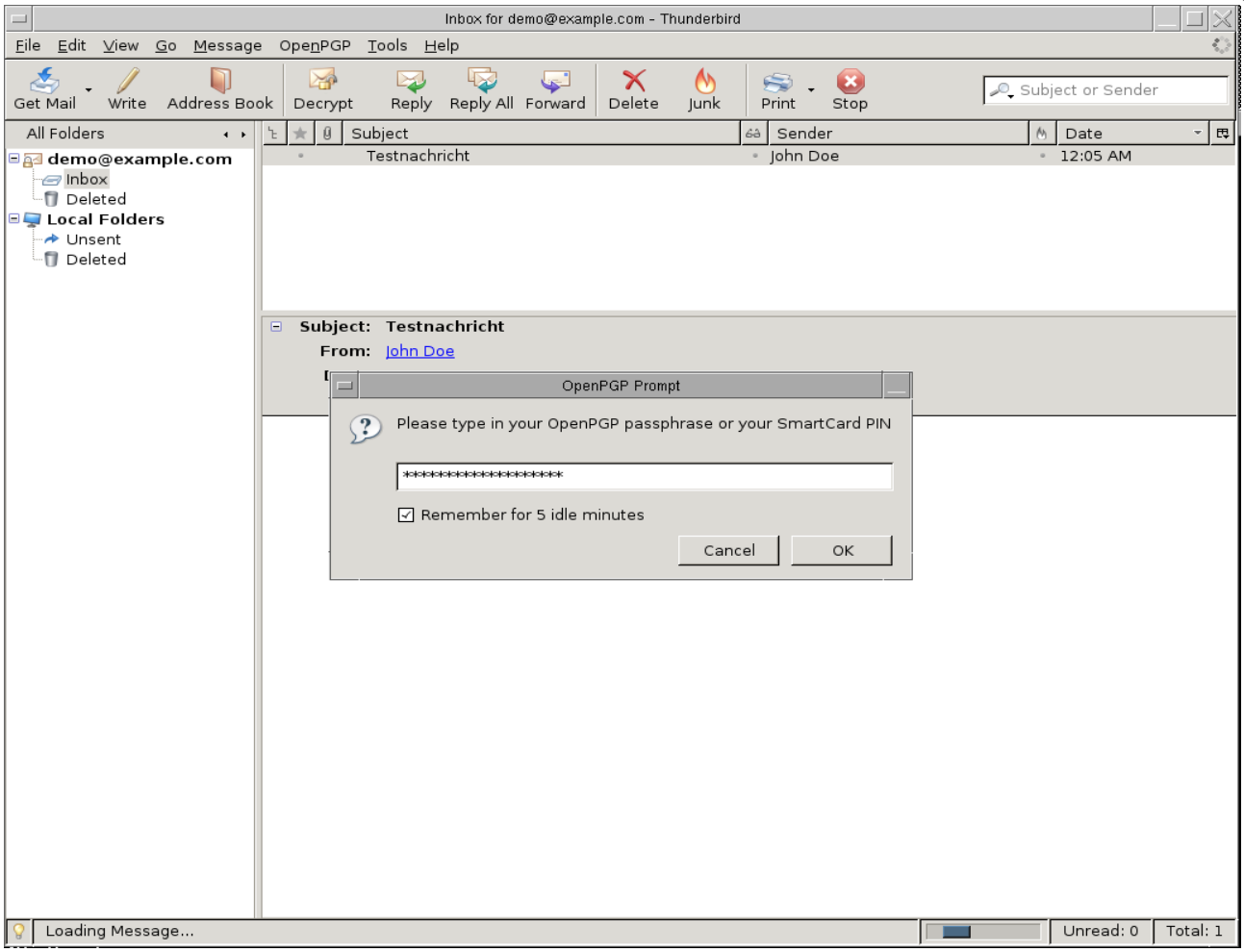
Damit ist der Versand der Nachricht abgeschlossen.

Empfang von Nachrichten

Die Nachricht wird von Ihrem Mailprogramm wie jede andere Nachricht auch behandelt. Auch wenn Sie die Nachricht nicht lesen könnten, könnten Sie sie doch hin- und herkopieren, weiterleiten, oder löschen.

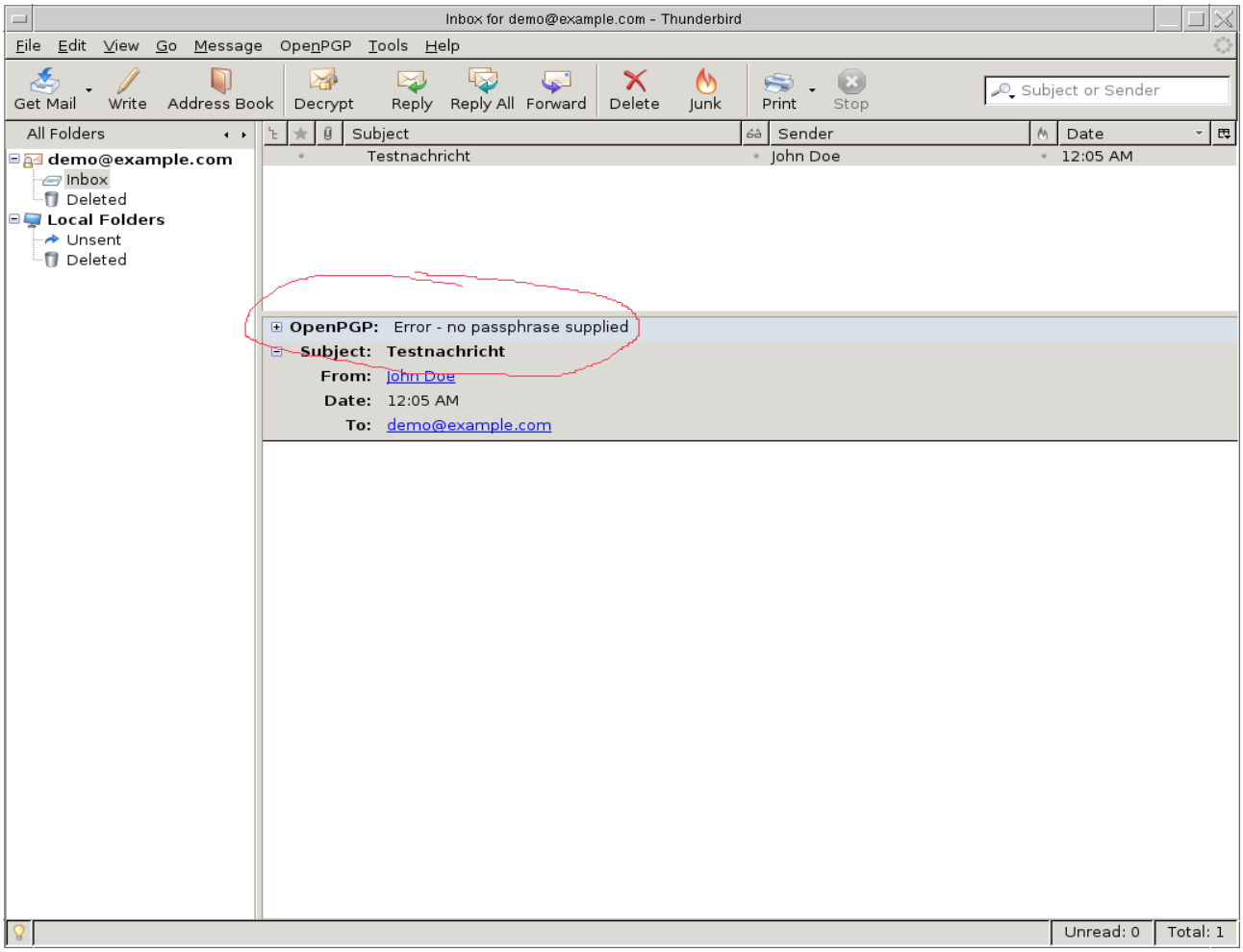
Wir finden die Nachricht in unserer Mailbox und werden nach der Passphrase gefragt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



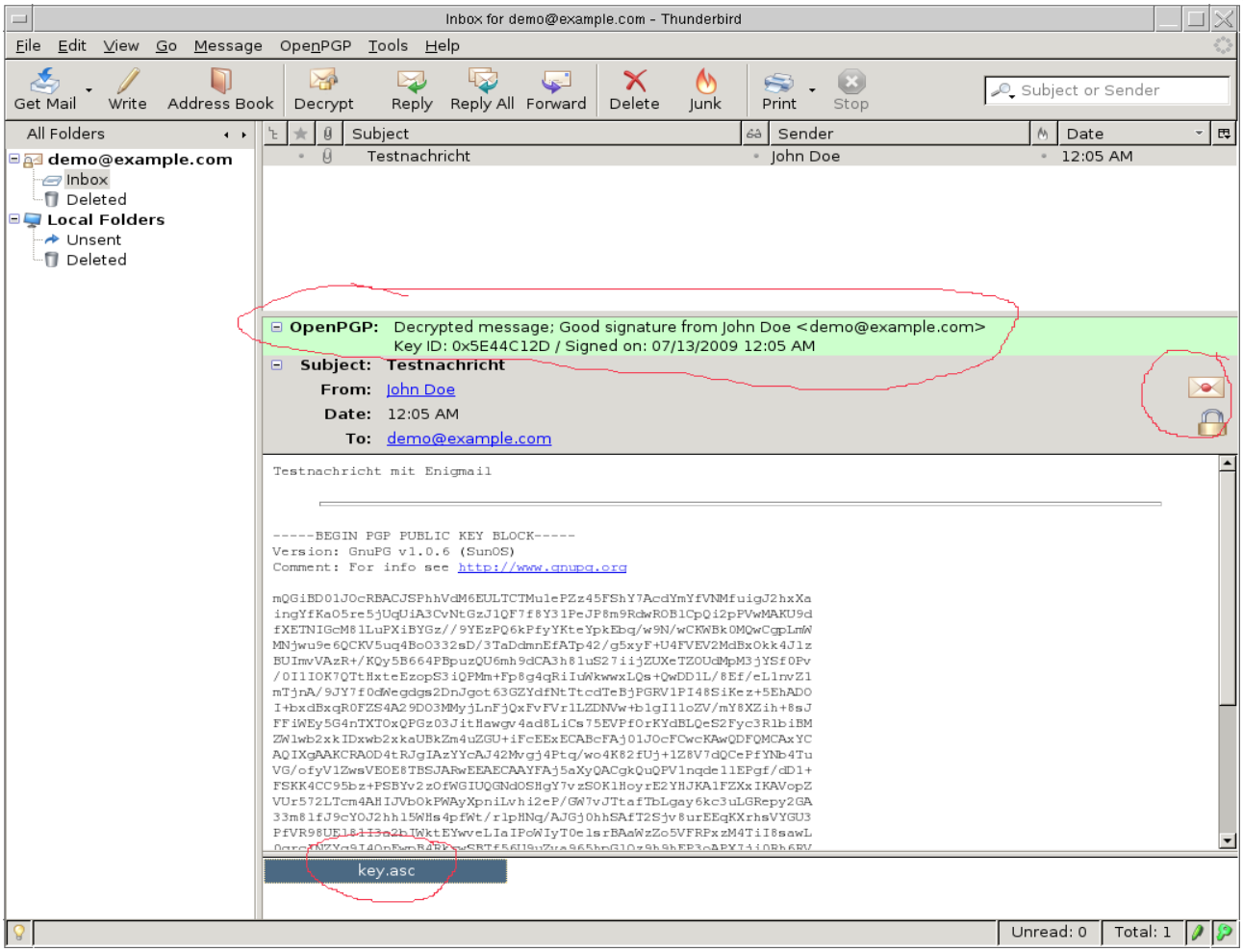
Wenn wir keine Passphrase eingeben, wird eine entsprechende Fehlermeldung angezeigt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



Geben wir stattdessen die richtige Passphrase ein, wird die Nachricht zusammen mit Informationen, die aus der Verschlüsselung stammen, angezeigt:

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364



In dem grünen Balken werden Absender, Schlüssel-ID, sowie Datum und Uhrzeit angezeigt. Unter der eigentlichen Nachricht wird der Anhang angezeigt. Da es sich in unserem Fall nur um eine Textdatei handelt, wird diese oben gleich als Vorschau mit angezeigt. Bei der angehängten Textdatei handelt es sich übrigens um die Textdarstellung eines OpenPGP-Schlüssels. Rechts sehen Sie noch ein Icon, das aus einem Briefumschlag und einem Vorhängeschloß besteht. Wenn Sie auf diesen Knopf drücken, öffnet sich ein Dialog mit Zusatzinformationen hinsichtlich des Schlüssels.

Damit sind die Grundfunktionen der Bearbeitung von verschlüsselten Emails erklärt.

Benutzungshinweise

Um von Systemen wie OpenPGP zu profitieren, müssen Sie einige Grundregeln im Umgang mit OpenPGP beachten.

1. **Zitieren Sie nie in einer unverschlüsselten Email aus einer verschlüsselten Email!** Wenn Sie es doch tun, schwächen Sie damit den oder die Schlüssel, mit dem oder denen die ursprüngliche Email verschlüsselt wurde.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364

2. Eine verschlüsselte Email sollte digital signiert werden. Das gehört zum guten Ton und trägt insgesamt dazu bei, die Akzeptanz des Systems zu erhöhen, da Sie Ihrem Kommunikationspartner damit einen Mehrwert bieten.
3. Sie sollten möglichst daran arbeiten, Ihre(n) Schlüssel von vielen Leuten unterschreiben zu lassen und selbst anderer Leute Schlüssel unterschreiben. Dieses Thema („Keysigning“) geht allerdings deutlich über diese Kurzanleitung hinaus.

Bei Fragen zu dieser Anleitung, oder allgemein zu unseren Themen, stehen wir Ihnen gerne zur Verfügung.

Zum Hochwald 20 http://www.oeko.net Inhaber: Dip..-Inf. Toni Müller gegründet 1993
D-51674 Wiehl AS29394 Dipl.-Ing. Imke Brandt online seit 1994
Tel. +49 2261 979364