

Installation und Konfiguration von Thunderbird in Kombination mit Enigmail

Inhaltsverzeichnis

Installation und Konfiguration von Thunderbird in Kombination mit Enigmail.	1
Lizenzbestimmungen	1
Zielsetzung	1
Umfang	2
Voraussetzungen	2
Grundlagen der Email-Verschlüsselung	2
Begriffsbestimmung	2
Verfahrensübersicht	3
Einrichtung	3
Nutzung (Übersicht)	3
Installation von Enigmail	4
Einrichtung von GnuPG und Enigmail	15
Erzeugung eines Schlüsselpaares	17
Allgemeine Einstellungen.	29
Versand von Emails	32
Empfang von Nachrichten	34
Benutzungshinweise	37
5	

Autor: Toni Müller

Stand: 13.07.2009

Lizenzbestimmungen

Dieser Text und die darin enthaltenen Bilder sind ©2009 <u>Öko.neT Müller &</u> <u>Brandt</u>, und können gemäß folgender Lizenz verwendet werden:



http://creativecommons.org/licenses/by-nc-sa/3.0/de/

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

IT-Consulting	IT-Security	Softwa	Softwareentwicklung Systemadministration				ration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postg	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	: Dip	Inf. Toni Müller	ç	egründet 1993
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	c	online seit 1994
Tel. +49 2261 979364								

Ôko.neT müller & brandt gbr

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 <u>Thunderbird</u> Version 2.x und <u>GnuPG</u> 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.

IT-Consulting	IT-Security	Softwa	Softwareentwicklung Systemadn			emadminist	ration	Hosting
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgi	reSQL
Zum Hochwald 20	http://w				r: Dip	oInf. Toni Müller	egründet 1993	
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	c	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.

IT-Consulting	IT-Security	Softwa	areentwicklung Systemadminist				ration	Hosting
Debian	OpenBSD	Plone	Zope	Pyt	hon	Perl	Postg	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	: Dip	Inf. Toni Müller	Q	egründet 1993
D-51674 Wiehl	AS2939	4			Dip	IIng. Imke Brandt	c	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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadminist				ration	Hosting	
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgi	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	r: [DipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			[DiplIng. Imke Brandt	C	online seit 1994
Tel. +49 2261 979364								



		manor a pranac
	demo@example.com - Thunderbird	
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>G</u> o <u>M</u> essage :	<u>I</u> ools <u>H</u> elp	0
Get Mail Write Address Book	Reply Reply All Forward Tag Delete Junk Print Back Forwards	🔎 Subject or Sender
All Folders 🔹	* Thursdankind Mail dam a @arram ala aam	
🛃 demo@example.com	Inunderbird Mail - demo@example.com	
🗄 🚽 Local Folders	Add-ons	
	Extensions Themas	
	Talkback 2.0.0.9 Sends information about program crashes to Mozilla.	
	Get Extensions	
	Search messages	
	y ocaren messages	
	Managa magazaga filtara	
	Y Manage message filters	
One		

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

IT-Consulting	IT-Security	Softwa	Softwareentwicklung			Systemadministration			
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgr	eSQL	
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Dip	Inf. Toni Müller	g	egründet 1993	
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	0	nline seit 1994	
Tel. +49 2261 979364									



müller & brandt gbr



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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadministr			tration Hosting	
Debian	OpenBSD	Plone	Zope	Pyth	on Perl	PostgreSQL
Zum Hochwald 20	http://ww	ww.oeko.net		Inhaber:	DipInf. Toni Müller	gegründet 1993
D-51674 Wiehl	AS29394	4			DiplIng. Imke Brandt	online seit 1994
Tel. +49 2261 979364						





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

IT-Consulting	IT-Security	Softwa	Softwareentwicklung System			emadminist	Hosting	
Debian	OpenBSD	Plone	Zope	Pyt	hon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	• http://www.oeko.net		Inhaber:	: D	ipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	1			D	iplIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								





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

IT-Consulting	IT-Security	Softwa	reentwick	klung Systemadministra			ration	Hosting
Debian	OpenBSD	Plone	Zope	Pyt	thon	Perl	Postgi	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	:	DipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4				DiplIng. Imke Brandt	C	nline seit 1994
Tel. +49 2261 979364								





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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadminist			tration Hosti	ing	
Debian	OpenBSD	Plone	Zope	Pyth	on Perl	PostgreSQL	
Zum Hochwald 20	http://ww	ww.oeko.net		Inhaber:	DipInf. Toni Müller	gegründet 19	993
D-51674 Wiehl	AS29394	1			DiplIng. Imke Brandt	online seit 19	994
Tel. +49 2261 979364							



Search Add-ons :: Add-ons for Thunderbird - Mozilla Firefox									
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp 🍻		📑 • S • 🖻 • 🖉 🧐 🖓 🦂 🧚 🎡	🥴 💩 - 📇 🔅						
🔄 🐗 🧼 - 🎯 😒 🏠 🔨 🗈 - 嬦 Mozilla Corporation (US) https://addons.mozilla.org/en-US/	hunderbir	rd/search?q=&cat=1%2C66	<u>☆</u> • ► • •						
<mark>⊖ · &</mark> · <u>□</u> · <u>■</u> · 0 · ⁽) · <i>∕</i> · ¹ / ₂ · <i>∕</i> · <u>₽</u> · <i>∕</i> ·			 ✓ ● 						
🖌 NginxHttpCoreModule 💿 🕞 Redmine - Download - Redm 💽 🎑 RubyForge: Redmine	Project	💽 🤹 Search Add-ons :: Add-ons f 💽	- 🗷						
NginxHttpCoreModule Mozilla Addd-ons for Opening enigmail-0.95.7-tb+sm.xpi You have chosen to open enigmail-0.95.7-tb+sm.xpi which is a: XPI file from: https://addons.mozilla.org What should Firefox do with this file? Open with Browse OpenPGP message entry ****** 24 reviews by Jeremy Gillick SwitchProxy Tool by Jeremy Gillick SwitchProxy Tool by Jeremy Gillick Sender Verification Anti-Phishing Extension	ow on.	Search Add-ons :: Add-ons f Register or Log in Other Applic vacy and Security Advanced - Advanced - (+ Download Now recommended + Download Now	ations -						
Protects you from phishing attacks by verifying the From: address domain name of em DNS-based reputation lists are used. ****** 8 reviews 567 weekly downloads Image: Secrit Bork Bork Bork! by Snert The Swedish Cheft travesty filter and URL blocker. View web pages or mail as spoken I spukee by zee Svedeesh Cheff." ****** 14 reviews 574 weekly downloads	ails as you	read them. Sender Policy Framework (SPF) and							
Done	۰ 💰	addons.mozilla.org 🚔 🐳 💿 FoxyProxy: Dis	abled 🛞 S 🔤 🖉						

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…":

IT-Consulting	IT-Security	Softwareentwicklung			Sys	Hosting		
Debian	OpenBSD	Plone Zope		Python Pe		Perl	PostgreSQL	
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	r:	DipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	4				DiplIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								

Öko.neT

demo@example.com - Thunderbird	
<u>File Edit V</u> iew <u>G</u> o <u>M</u> essage <u>T</u> ools <u>H</u> elp	0 ⁰ 0 0,0
Get Mail Write Address Book Reply All Forward Tag Delete Junk Print Back Forwards	₽ Subject or Sender
All Folders	
Select an extension to install	
Location: enigmail-0.95.7-tb+sm.xpi	
Places Name ,	▼ Modified
🔍 Search 🛅 gconfd-root	Today at 13:29
🛞 Recently Used 🛅 gconf.	Today at 12:31
a orbit-root	Today at 13:29
🖾 Desktop 🛅 orbit	Today at 13:44
File System	Today at 12:30
tmp 🚺 💾 enigmail-0.95.7-tb+sm.xpi	Today at 13:54
	· · · · · · · · · · · · · · · · · · ·
	Extensions (*.xpi)
28	Cancel Den
9 Done	

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.

IT-Consulting	IT-Security	Softwareentwicklung		lung S	ystemadminist	ration Hosting
Debian	OpenBSD	Plone	Zope	Pyth	on Perl	PostgreSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber:	DipInf. Toni Müller	gegründet 1993
D-51674 Wiehl	AS29394	4			DiplIng. Imke Brandt	online seit 1994
Tel. +49 2261 979364						





IT-Consulting IT-Security Softwareentwicklung Systemadministration Hosting Debian **OpenBSD** Plone Zope Python Perl PostgreSQL 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



	indio: d brandt
demo@example.com - Thunderbird	
Eile Edit View Go Message Tools Help	<u></u>
Get Mail Write Address Book Reply All Forward Tag Delete Junk Print Back Forwards	🔎 Subject or Sender
All Folders	
I hunderbird Mail - demo@example.com	
Exten You have asked to install the following item:	
enigmail-0.95.7-tb+sm Unsigned	
from: file:///tmp/enigmail-0.95.7-tb+sm.xpi	
Malicious software can damage your computer or violate	
You should only install software from sources	
that you trust.	
Cancel Install Now	
ins risions	
Search messages	
Manage message filters	
♀ Done	

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

IT-Consulting IT-Security		Softwareentwicklung			Syst	Hosting		
Debian	OpenBSD	Plone	Zope	Pyt	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://www.oeko.net			Inhaber	: [DipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			[DiplIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



	demo@example.com - Thunderbird	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essage	<u>T</u> ools <u>H</u> elp	\diamond
Get Mail Write Address Book	Reply Reply All Forward Tag Delete Junk Print Back Forwards	₽, Subject or Sender
All Folders	Thunderbird Mail - demo@example.com	
	Add-ons	
	Extensions Themes Installation	
	Enigmail 0.95.7 Restart to complete the installation.	
	Search messages	
	Manage message filters	
One	I	





Einrichtung von GnuPG und Enigmail

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

	\sim	Mozilla Thunderbird		
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essa	age Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp			0 ⁰ 0 000
Get Mail Write Address	Boon Decrypt Reply Re	Ny All Forward Delete Junk Print	Stop	der
All Folders				
🔤 demo@example.com	_			
O Done				

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:

IT-Consulting	IT-Security	Softwareentwicklung			Syste	Hosting		
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgi	reSQL
Zum Hochwald 20	http://w	http://www.oeko.net			r: Dip	oInf. Toni Müller	egründet 1993	
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	c	online seit 1994
Tel. +49 2261 979364								



	Mozilla Thunderbird	
	Tools Help	
Get Mail Write Address Book Decrypt	Reply Reply All Forward Delete Junk Print Stop	🔎 Subject or Sender
All Folders 🔹		
ademo@example.com	OpenPGP Preferences	
	Basic	
	Basic Settings	
	Ciles and Directories	
1	GnuPG was found in /usr/bin/gpg	
	Override with Browse	
	Passphrase settings	
	Remember passphrase for 5 minutes of idle time	
	Never ask for any passphrase	
	· · · · · · · · · · · · · · · · · · ·	
	Display expert settings	
	Reset	
	Cancel OK	
♀ Done		

- 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.
- In dem Feld "Passphrase-Einstellungen" kann man einstellen, wie lange die Passphrase¹ halten soll. Hier kann man einen Mittelwert zwischen Bequemlichkeit und Sicherheit wählen, allerdings sollte man das Feld "Nie nach der Passphrase fragen" <u>NIE</u> 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.

IT-Consulting	IT-Security	Softwareentwicklung			Syste	Hosting		
Debian	OpenBSD	BSD Plone Zope Python		Perl	Postgr	eSQL		
Zum Hochwald 20	http://www.oeko.net			Inhaber	: Dip	Inf. Toni Müller	egründet 1993	
D-51674 Wiehl	AS2939	4			Dip	IIng. Imke Brandt	0	nline 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:

	Mozilla Thundi	erbird	
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>G</u> o <u>M</u> essage	Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp		0
Get Mail Write Address Book	<u>D</u> ecrypt/Verify <u>S</u> ave Decrypted Message	ete junk Print Stop	₽, Subject or Sender
All Folders	✓ <u>A</u> utomatically Decrypt/Verify Messages		
ademo@example.com ∎ 🚽 Local Folders	Clear Saved Passphrase R <u>e</u> load Message Sender's <u>K</u> ey →		
	Preferences		
	Edit Per- <u>R</u> ecipient Rules		
	Key Management		
	<u>M</u> anage SmartCard		
	Debugging OpenP <u>G</u> P •		
	<u>H</u> elp		
	A <u>b</u> out OpenPGP		
Dane			
V Done			

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":

IT-Consulting IT-Security		Softwareentwicklung			Syst	Hosting		
Debian	OpenBSD	Plone	Zope	Pyt	hon	Perl	Postgr	reSQL
Zum Hochwald 20	http://www.oeko.net			Inhaber	: D	ipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			D	iplIng. Imke Brandt	0	online seit 1994
Tel. +49 2261 979364								



Eile Edit View Go Message OpenPGP Tools Help Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Print Stop All Folders Image: Stop Image: Stop Image: Stop Image: Stop Subject or Sender Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop <t< th=""><th></th></t<>	
Get Mail Write Address Book Decrypt Reply Reply Reply Reply All Forward Delete Junk Print Stop All Folders <t< th=""><th></th></t<>	
All Folders	
A demo@example.com	
OpenPGP Key Management Eile Edit View Keyserven Generate Filter for user ID's or key ID's containing: Clear Account / User ID Key ID Type Key V Expiry	
Filter for user ID's or key ID's containing:	
Account / User ID Key ID Type Key V Owne Expiry R	
Done	

IT-Consulting	IT-Security	Softwareentwicklung Systemadministra			ration	Hosting		
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Di	ipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394				DiplIng. Imke Brandt			nline seit 1994
Tel. +49 2261 979364								

		Mozilla	Thunderbird		
<u>F</u> ile <u>E</u> dit ⊻iew <u>G</u> o <u>M</u>	lessage Ope <u>n</u> PGP	<u>T</u> ools <u>H</u> elp			500 B
Get Mail Write Addre	ess Book	Reply Reply All Forwa	rd Delete Junk	Si v Stop	✓ Subject or Sender
All Folders	< >				
ademo@example.c ≇ 🚽 Local Folders	om				
		OpenPGF	Key Management		
	<u>E</u> ile <u>E</u> dit ⊻iew <u>I</u>	eyserver <u>G</u> enerate			
	Filter for user ID's o	r key ID's o New <u>K</u> ey Pair		<u>C</u> lear	
		<u> </u>	ertificate		
	Account / Oser it		кеуло туре	Key V Owne Exp	
💡 Done					

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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadministratio			ration	Hosting		
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	: Dip.	Inf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	4			Dipl	Ing. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



Mapillo Thur dashind	
File Edit View Ge Message OpenPGP Teals Help	
Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Pri	The stop Subject or Sender
All Folders • •	
a demo@example.com ♣ ↓ Local Folders	
OpenPGP Key Management	
Elle Edit View Keyserv Generate OpenPGP	'Key
Filter for user ID's or key IC Account / User ID John Doe <demo@example.com> - demo@exar</demo@example.com>	nple.com
Account / User ID 🛛 Use generated key for the selected identity	
□ No passphrase	
Passphrase Passphrase (repeat)	
Comment	
Key expiry Advanced C	
Key expires in 5 years 🗧 🗅 Key does not expire	
Generate key Cancel	4
Key Generation Console NOTE: Key generation may take up to several minutes to generation is in progress. Actively browsing or performing disk-inter the 'randomness pool' and speed-up the process. You will be alerte	complete. Do not exit the application while key nsive operations during key generation will replenish d when key generation is completed.
♀ Done	

1. Sie werden zur zweimaligen Eingabe einer sogenannten "Passphrase" aufgefordert. Bei der Passphrase handelt es sich guasi 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).

IT-Consulting	IT-Security	Softwareentwicklung S			Syste	Hosting		
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgi	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Dip	Inf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	C	online seit 1994
Tel +49 2261 979364								

Ôko.neT müller & brandt abr

- 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:

IT-Consulting	IT-Security	Softwareentwicklung Systemad			emadminist	administration Hosti		
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	r: Di	pInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Di	plIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



	Generate OpenPGP Key							
Account / User ID John Doe < demo@example.com> - demo@example.com (*)								
☑ Use generated key for the selected identity								
🗌 No passphrase								
Passphrase ***************	Passphrase (repeat) ************							
Comment								
Key expiry Advanced								
Key size 2048 😫								
Key type RSA								
Generate key Cancel								
Key Generation Console								
NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.								

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:

IT-Consulting	IT-Security	Softwareentwicklung		Syste	Hosting			
Debian	OpenBSD	Plone	Zope	Pyt	hon	Perl	Postgi	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber:	Dip	Inf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Dip	IIng. Imke Brandt	C	nline seit 1994
Tel. +49 2261 979364								



	Mozilla Thunderbird	
	<u>T</u> ools <u>H</u> elp	<u> </u>
Get Mail Write Address Book Decrypt	Reply All Forward Delete Junk	, Subject or Sender
All Folders 🔹 🔸		
Image: Second s		
	enPGP Key Management	
Eile Edit View Keyserv	Generate OpenPGP Key	
Filter for user ID's or key IC Account / Us	er ID John Doe <demo@example.com> - demo@example.com</demo@example.com>	[‡]
Account / User ID 🗹 Use gen	erated key for the selected identity	
□ No passph	rase	
Passphrase	**************************************	
Comment		
Key expiry A	dvanced	
	OpenPGP Confirm	
Key expires	in 5 Generate public and private keys for 'John Doe <demo@example< td=""><td>e.com>'?</td></demo@example<>	e.com>'?
		Y
Generate ke	y Cancel	
		່ວ
Key Genera	tion Console	Z
NOTE: Key	generation may take up to several minutes to complete. Do not exit this is progress. Actively browsing or performing disk-intensive operations during k	he application while key
the 'random	iness pool' and speed-up the process. You will be alerted when key generation is	completed.
V Done		

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

IT-Consulting	IT-Security	Softwareentwicklung			Syst	Hosting		
Debian	OpenBSD	Plone	Zope	Pyt	hon	Perl	Postgr	eSQL
Zum Hochwald 20	http://ww	ww.oeko.net		Inhaber	: [DipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	1			I	DiplIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



🖂 Mozilla Thunderbird	
<u> E</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essage Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp	\diamond
Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Print Stop	₽, Subject or Sender
All Folders · ·	
a demo@example.com € 晕 Local Folders	
🗆 OpenPGP Key Management 🔄 🗔 🔀	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>K</u> eyserver <u>G</u> enerate	
Filter for user ID's or key ID's containing:	
Account / User ID Key ID Type Key V Owne Expiry 🛤	
John Doe <demo@example.com> 5E44C12D pub/sec ultimate ultimate 07/17/</demo@example.com>	
Q Done	

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:

IT-Consulting	IT-Security	Softwa	reentwick	lung	Systemadminist		ministration Ho	
Debian	OpenBSD	Plone	Zope	Pyt	hon	Perl	Postg	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber:	Dip	Inf. Toni Müller	ç	gegründet 1993
D-51674 Wiehl	AS2939	4			Dip	Ing. Imke Brandt	c	online seit 1994
Tel. +49 2261 979364								



	Mozilla Thunderbird	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essage Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp		
Get Mail Write Address Book Decrypt Reply Reply	All Forward Delete Junk Print Stop	🔎 Subject or Sender
All Folders 🔹 🔸		
a demo@example.com € 🖵 Local Folders		
DpenPGP Key Managel	ment 📃 🗔 📈	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>K</u> eyserver <u>G</u> enerate		
Filter for user ID's or key ID's containing:	Clear	
Account / User ID Key ID	Type Key V Owne Expiry 🖪	
John Doe < demo@example.com> 5E44C12D	Copy Public Keys to Clipboard Export Keys to File Send Public Keys by Email Upload Public Keys to Keyserver Refresh Public Keys From Keyserver Sign Key Set Owner Trust Disable Key Revoke Key Delete Key Manage User IDs Change Passphrase Generate & Save Revocation Certificate View Signatures View Photo ID Key Properties	
Image: Constraint of the second sec		

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:

IT-Consulting	IT-Security	Softwa	reentwick	lung	Systemadministrat		ration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	: D	ipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			D	iplIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



Mozilia Thunderbird	
Eile Edit View Go Message OpenPGP Tools Help	0
Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Stop	🔎 Subject or Sender
All Folders · ·	
ademo@example.com	
e local Folders	
Copenrar Key Management	
Account / User ID Key ID Type Key V Owne Expiry 🛱	
John Doe <demo@example.com> 5E44C12D pub/sec ultimate ultimate 07/17/</demo@example.com>	
OpenPGP Prompt	
Please type in your OpenPGP passphrase or your SmartCard PIN	
Cancel OK	
♀ Done	

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

IT-Consulting	IT-Security	Softwa	reentwick	lung	Systemadministratio		ration	Hosting
Debian	OpenBSD	Plone	Zope	Ру	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	: Dip.	Inf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	4			Dipl	Ing. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



A Mozilla Thunderbird	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essage Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp	0
Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Print Stop	🔎 Subject or Sender
All Folders ••	
🚰 demo@example.com	
🖲 📮 Local Folders	
<u>File Edit View K</u> eyserver <u>G</u> enerate	
Filter for user ID's or key ID's containing:	
Account / User ID Key ID Type Key V Owne Expiry 🖽	
John Doe <demo@example.com> 5E44C12D pub/sec ultimate ultimate 07/17/</demo@example.com>	
OpenPCP Alert	
The revocation certificate has been successfully created. You can use it to invalidate your	
public key, e.g. in case you would lose your secret key.	
Please transfer it to a medium which can be stored away safely such as a CD or Floppy Disk.	
If somebody gains access to this certificate they can use it to render your key unusable.	
ОК	
Image: Construction of the second s	

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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadmi		ystemadminist	ration Hosting	
Debian	OpenBSD	Plone	Zope	Pytho	n Perl	PostgreSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber:	DipInf. Toni Müller	gegründet 1993
D-51674 Wiehl	AS2939	4			DiplIng. Imke Brandt	online seit 1994
Tel +49 2261 979364						



Elie Edit View Go Message OpenPGP Tools Help Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk Print Stop Subject or Sender All Folders Cocal Folders OpenPGP Key Management Elie Edit View Keyserver Generate Filter for user ID's Befresh Selected Public Keys Search for Keys Account / User Upload Public Keys Type Key V Owne Expiry C John Doe < Refresh All Public Keys 2D pub/sec ultimate ultimate 07/17/	
Get Mail Write Address Book Derypt Reply Reply All Forward Delete Junk Print Stop All Folders	
All Folders	
<pre>demo@example.com Local Folders OpenPGP Key Management File Edit View Keyserver Generate Filter for user ID's Befresh Selected Public Keys Search for Keys Yupload Public Keys Account / User Upload Public Keys 2D pub/sec ultimate ultimate 07/17/</pre>	
Clear File Edit View Keyserver Generate Filter for user ID's Befresh Selected Public Keys Search for Keys Search for Keys Account / User Upload Public Keys Type Key V Owne Expiry Refresh All Public Keys 2D pub/sec ultimate 07/17/	
Eile Edit View Keyserver Generate Filter for user ID's Befresh Selected Public Keys Clear Search for Keys Type Key V Owne Account / User Upload Public Keys Type Key V John Doe <c< td=""> Refresh All Public Keys 2D pub/sec ultimate 07/17/</c<>	
Filter for user ID's Befresh Selected Public Keys Search for Keys Type Account / User Upload Public Keys John Doe <c< td=""> Refresh All Public Keys 2D pub/sec ultimate 07/17/</c<>	
Account / User Upload Public Keys Type Key V Owne Expiry R John Doe <c 07="" 17="" 2d="" <="" all="" keys="" pub="" public="" refresh="" sec="" td="" ultimate=""><td></td></c>	
John Doe <c <u="" refresh="">All Public Keys 2D pub/sec ultimate ultimate 07/17/</c>	
Image:	

IT-Consulting	IT-Security	Softwa	reentwick	lung	Systemadministratio		ration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	r: Di	pInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	4			Di	plIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



🗆 Mozilla Thunderbird	
<u>Eile E</u> dit ⊻iew <u>G</u> o <u>M</u> essage Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp	() ()
Set Mail Write Address Book Image: Comparison of the provided in the	🔎 Subject or Sender
All Folders · ·	
실 demo@example.com 면 및 Local Folders	
DenPGP Key Management	
<u>File Edit View K</u> eyserver <u>G</u> enerate	
Filter for user ID's or key ID's containing:	
Account / User ID Key ID Type Key V Owne Expiry 🛱	
John Doe <demo@example.com> 5E44C12D pub/sec ultimate ultimate 07/17/</demo@example.com>	
Select Keyserver	
Send public key 0x5E44C12D - John Doe	
<demo@example.com> to keyserver:</demo@example.com>	
Reyserver pool.sks-keyservers.net	
subkeys non net	
pgp.mit.edu	
ldap://certserver.pgp.com	

Da die Keyserver unterschiedlich gut verfügbar, aber unterereinander 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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadministrat		Systemadministr		ration	Hosting	
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgi	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Dip	Inf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	o	nline 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:

IT-Consulting	IT-Security	Softwareentwicklung Systemadministra		Softwareentwick		Systemadministr		ration	Hosting
Debian	OpenBSD	Plone	Zope	Pyth	on	Perl	Postgr	eSQL	
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber:	Dip	-Inf. Toni Müller	g	egründet 1993	
D-51674 Wiehl	AS29394	4			Dipl.	-Ing. Imke Brandt	0	nline seit 1994	
Tel. +49 2261 979364									



		Account Settings
■ dem Sei Coj Dis Jun Coal Den Sei Local Dis Jun Outgo	o@example.com rver Settings pies & Folders mposition & Addressing to Space k Settings enPGP Security curity Folders to Space k Settings bing Server (SMTP)	OpenPGP Options (Enigmail) Support for OpenPGP encryption and signing messages is provided by Enigmail. You need to have GnuPG (gpg) installed in order to use this feature. Image: Enable OpenPGP support (Enigmail) for this identity Image: Enable OpenPGP support (Enigmail) for this identity to identify OpenPGP key Image: Enable OpenPGP demassages by default Image: Encrypt messages by default Imag
	<u>A</u> dd Account	
	Set as De <u>f</u> ault	
	<u>R</u> emove Account	
		Cancel OK

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.

IT-Consulting	IT-Security	Softwa	reentwick	lung	Syste	madminist	ration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgi	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Dip	Inf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Dip	lIng. Imke Brandt	0	nline 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.

IT-Consulting	IT-Security	Softwa	reentwick	lung	Syste	emadminist	tration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgi	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Dij	pInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Di	plIng. Imke Brandt	c	online seit 1994
Tel +49 2261 979364								



- Common Technologiak	
Compose: lestnachricht Compose: lestnachricht	
Send Contacts Spell Attach OpenPGP S/MIME Save	
From: John Doe <demo@example.com> < Sign Message Ctrl+Shift+S + Attachr</demo@example.com>	nents:
To: I demo@example.con	ic .
Ignore Per-Recipient OpenDGP (Epigmail) security settings	
Subject: Testnachricht	
Body Text $[\div]$ Fixed Width $[\div]$ \blacksquare A^* A^* B I \underline{U} $!= \frac{1}{2}$ $!= != != != != != != != != != != != != !$	
Testnachricht mit Enigmail	
]

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:

IT-Consulting	IT-Security	Softwa	reentwick	lung	Syste	emadminist	ration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgi	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	r: Di	pInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			Di	plIng. Imke Brandt	C	nline seit 1994
Tel. +49 2261 979364								



Compose: Testnachricht	
<u>Eile Edit V</u> iew Insert F <u>o</u> rmat O ptions Ope<u>n</u>PGP <u>T</u>ools <u>H</u>elp	\sim
Send Contacts Spell Attach OpenPGP S/MIME Save	
F <u>r</u> om: John Doe <demo@example.com> - demo@example.com 🛟</demo@example.com>	Attachments:
To: 45 demo@example.com	key.asc
Subject: Testnachricht	
Body Text Fixed Width \checkmark A^* B I U \blacksquare 1 U 1 <td></td>	
Testnachricht mit Enigmail	
OpenPGP Prompt	
Please type in your OpenPGP passphrase or your SmartCard PIN	
*0000000000000000	
☑ Remember for 5 idle minutes	
Creating mail message	

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:

IT-Consulting	IT-Security	Softwa	reentwick	lung	Syste	emadminist	ration	Hosting
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postg	reSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhabe	r: Dij	Inf. Toni Müller	ç	egründet 1993
D-51674 Wiehl	AS29394	4			Dij	olIng. Imke Brandt	c	online seit 1994
Tel +49 2261 979364								



	Inbox for demo@example.com - Thunderbird	
File Edit View Go Message		
Get Mail Write Address Boo	ok Decrypt Reply Reply All Forward Delete Junk Print Stop	Subject or Sender
All Folders 🔹 🔸	눈 🚖 🛛 Subject 64 Sender	🗄 Date 🗸 🖽
 a demo@example.com Inbox Deleted Local Folders ✓ Unsent ① Deleted 	Testnachricht John Doe Subject: Testnachricht	- 12:05 AM
	From: John Doe	
	OpenPGP Prompt	
	Please type in your OpenPGP passphrase or your SmartCard PIN ***********************************	
W Loading Message		Unread: 0 Total: 1

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

IT-Consulting	IT-Security	Softwareentwicklung Systemadminist		ration	Hosting			
Debian	OpenBSD	Plone	Zope	Py	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	r: Di	pInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS29394	4			Di	plIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>G</u> o <u>M</u> essag	e Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp		O 100 Control 1
Get Mail Write Address Bo	ok Decrypt Reply Reply All Forward Delete	Junk Print Stop	🔎 Subject or Sender
All Folders 🔹 🔸	눈 ★ 🖉 Subject	68 Sender	\land Date 👻 🖽
All Folders • •	OpenPGP: Error - no passphrase supplied Subject: Testnachricht Subject: Testnachricht From: john Doe Date: 12:05 AM To: demo@example.com	j& Sender - John Doe	M_ Date ~ [13] - 12:05 AM
8			Unread: 0 Total: 1

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

IT-Consulting	IT-Security	Softwa	reentwick	lung	Syst	emadminist	ration	Hosting
Debian	OpenBSD	Plone	Zope	Pyt	thon	Perl	Postgr	eSQL
Zum Hochwald 20	http://w	ww.oeko.net		Inhaber	: [DipInf. Toni Müller	g	egründet 1993
D-51674 Wiehl	AS2939	4			[DiplIng. Imke Brandt	0	nline seit 1994
Tel. +49 2261 979364								



	Inbox for demo@example.com -	Thunderbird	
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>G</u> o <u>M</u> essage	Ope <u>n</u> PGP <u>T</u> ools <u>H</u> elp		()
Get Mail Write Address Boo	k Decrypt Reply Reply All Forward Delete	🔥 🥯 - 🛞 Junk Print Stop	Subject or Sender
All Folders 🔹 🔸	눈 ★ 🖉 Subject	68 Sender	\land Date 👻 🖽
 a demo@example.com Inbox Deleted Local Folders ✓ Unsent Deleted 	OpenPGP: Decrypted message; Good signatu Key ID: 0x5E44C12D / Signed on: 0 Subject: Testnachricht Form: Jobs Dec	• John Doe re from John Doe <demo@example 7/13/2009 12:05 AM</demo@example 	• 12:05 AM
	From: <u>John Doe</u> Date: 12:05 AM To: <u>demo@example.com</u>		
	Testnachricht mit Enigmail BEGIN FGP PUBLIC KEY BLOCK Version: GnuPG v1.0.6 (SunOS) Comment: For info see <u>http://www.gnupg.org</u> mQGiBD01J0cRBACJSPhNVdM6EULTCTMulePZz45FShYAc ingYfRaOSre5jUgUA3CvNtGzJ0F718V31PcJP8mPRdeR MTyMu9e6QCKV5ug4Bo03322D/3TaDdnnEfATp42/gSxyF+ BUImvVaE+/KQv5B664PByu2OBMb9JLnF28dqRiluMXwwxLQs+ mTjnA/9JY1F0dWegdga2DnJgot63GZ4GtNtTtcdTeBjPGR HtbxdBxgH0FZSAA2903Mb9JLnF28g4QRiluMXwwxLQs+ mTjnA/9JY1F0dWegdga2DnJgot63GZ4GtNtTtcdTeBjPGR FFiWEy564nTXT0xQFC203JtHawgv4adBLiCs75EVFF0-K ZW1wb2xk1Dxwb2skaUBKZm4d2GU+FEE5EECABCF30107 AQIXgAAKCRA0D4EkJgIAzYtCAJ422Mvg14Eq/wo4K82fUj VG/ofyVIZwsVE0687BSJARwEEAECAAYFAj5AxVQACgkQuQ FSKK4CC95b2+FESHV2z0fWG1U0GNdOSHgY7wzSOKIHoyrE PUS572LTcm4AHJVb0KFWAyXpnitw12eF/GM7vJTtafTb 33m81f3geJ02Dh1MHs4pfWk/rjPNk0/AJG90hSAFT25 PfVR9UE181362hJQhtESymveLiaIPcMJyT0e1srBAMv2Z OurofW7X98140pBreR4BYDv5BFf56UBu7Zv965hnG10z9h	dYmYfVNMfuigJ2hxXa DBlCpQi2pFVwMARU9d VwCKMBKOMWoCqpLmN Q4FVEV2NdBxOkk4J1z X=TZOUdMpM3}Y5f0Fv QwDD1L/8Ef/eL1nvZ1 V1P14851K=z+55hADO 111c2V/nY8Zih+8sJ YdBLQ=S2Fyc3RlbiBM =FCwcKAwQDFQMCAxYC +1Z8V7dQC=PfYNb4Tu FV1ng4=1EPgf/dD1+ 2Y1hKA1FZXx1KAVopZ Lgay6kc3uLGRepy2GA Y8urEEgKXhsVYGU3 oSVFRPxzM4Ti18sawL ShEP1oAPYT410Ph6EV	
8			Unread: 0 Total: 1 🖉 👂

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.

IT-Consulting	IT-Security	Softwareentwicklung			Syste	Hosting		
Debian	OpenBSD	Plone	Zope	e Pytł		Perl	PostgreSQL	
Zum Hochwald 20	http://www.oeko.net			Inhaber:	Dip	Inf. Toni Müller	egründet 1993	
D-51674 Wiehl	AS2939	4			Dip	IIng. Imke Brandt	C	online seit 1994
Tel. +49 2261 979364								

Öko.neT müller & brandt gbr

- 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.

IT-Consulting	IT-Security	Softwareentwicklung			Syste	Hosting		
Debian	OpenBSD	Plone	Zope Py		thon Perl		PostgreSQL	
Zum Hochwald 20	http://www.oeko.net			Inhaber	: Dip	Inf. Toni Müller	egründet 1993	
D-51674 Wiehl	AS2939	4			Dip	olIng. Imke Brandt	c	online seit 1994
Tel. +49 2261 979364								