DS-GVO:

Datenschutz praktisch

Wie Sie ihre e-Mail Kommunikation effizient und wirksam verschlüsseln

Datenschutzbeauftragter (IHK)
Baden-Baden

Peter Dippold

DS-GVO

Datenschutz praktisch

Wie Sie ihre e-Mail Kommunikation

effizient und wirksam

verschlüsseln.

Inhaltsverzeichnis

Impressum

Datenschutzbeauftragter (IHK)
Peter Dippold
Eichelgartenstr. 6
76530 Baden-Baden

www.dsb-baden-baden.de
info@dsb-baden-baden.de

Dieses Werk darf kostenfrei kopiert, verbreitet, geteilt und auf sonstigen Wegen verbreitet werden, sofern es in seinen sämtlichen Teilen unverändert erhalten bleibt. Änderungen, Kürzungen oder Ergänzungen bedürfen der schriftlichen Zustimmung des Autors.

Dieses Buch ist bereits vor einigen Jahren entstanden und wurde 2018 überarbeitet. Möglicherweise entspricht der eine oder andere verwendete Begriff älteren Softwareversionen und ist bei der Korrektur durchgerutscht. Sollte dem so sein, bitte ich eventuelle Unannehmlichkeiten zu entschuldigen. Bitte melden Sie mir einen solchen Fehler zurück, damit ich eine verbesserte Version zur Verfügung stellen kann.

Lob und Kritik werden natürlich gern angenommen, auch wenn ich nicht immer dazu komme, jede Mail gleich zu beantworten.

Herzlichen Dank für Ihr Interesse

Vorwort

Eigentlich wussten wir es schon immer: Unsere Kommunikation via E-Mail ist offen und frei lesbar, für jeden, der Zugang zu den Systemen hat. Das hat uns lange nicht gestört, die meisten von uns jedenfalls, denn wir wähnten uns sicher in der Masse der Daten und was sollte denn speziell an unseren Daten für Dritte interessant sein?

Die Anhänge von Anwälten und anderen, die vertrauliche Informationen per Mail versenden und jeden Unbefugten auffordern, er möge diese Mail doch bitte sehr nicht lesen, wenn er nicht dazu berechtigt ist, haben schon oft Gelächter produziert, aber nichts am Umstand geändert. Nach wie vor sind derartige Disclaimer bei Anwälten und selbst großen Unternehmen gängig, man hat sich daran gewöhnt.

Mails mit personenbezogenen Daten, die nach Art. 9 DS-GVO in besonderer Weise (personenbezogene Daten besonderer Kategorien) geschützt sind, dürfen keinesfalls unverschlüsselt verschickt werden. Dies gilt sowohl für die Transportverschlüsselung mit TLS/SSL als auch für die Inhalteverschlüsselung. Ohne S-Mime oder PGP verschlüsselt ein klarer Verstoß gegen geltendes Recht, der zu recht mit hohen Bußgeldern belegt werden kann.

Mit Inkrafttreten der EU Datenschutzgrundverordnung (DS-GVO) und der Aktualisierung des Bundesdatenschutzgesetzes als BDSG (neu), beide gültig seit 25.5.2018 ist eine gewachsene Sensibilität, aber auch Verunsicherung im Umgang mit personenbezogenen Daten zu beobachten. Dabei sind viele der als neu empfundenen Regelungen in Wirklichkeit alte Hüte und waren auch schon in der Vergangenheit gesetzlich geregelt. Nur wirklich gekümmert, hat es keinen. Angesichts der Höhe der Bußgelder, die nun bei Verstößen gegen die DS-GVO und das BDSG (neu) verhängt werden können, dies ist eine der Neuerungen auf Gesetzesebene, ist diese Ignoranz nun Vergangenheit.

Sollten die aktuellen Entwicklungen dazu führen, dass eine breite Mehrheit künftig sensibler mit dem Thema Datensparsamkeit und Datenschutz umgeht, dann ist das bestimmt nicht zu unser aller Schaden.

In diesem kurzen Ratgeber möchte ich ihnen einen schon länger existierenden Weg, ihre Kommunikation per Email zu schützen, vorstellen und eine kleine Anleitung geben, wie sie das auf ihrem bestehenden PC-System umsetzen können. Voraussetzung hierfür ist ein PC mit einem aktuellen Betriebssystem, egal ob Linux, Windows oder Mac-OS. Alle hier vorgestellten Programme können sie kostenfrei beziehen, der Lernaufwand zum Umgang hält sich in Grenzen. Der Lohn für die Mühe ist das gute Gefühl, wenigstens die persönliche oder geschäftskritische Kommunikation besser geschützt zu haben.

Um Ihre Kommunikation per Mail zu verschlüsseln, benötigen Sie drei Programme:

- Thunderbird, ein kostenfreier, komfortabler Mailclient,
- GnuPG, die open source Variante von GPG,
- Enigmail, ein einfaches Add-on für Thunderbird.

Im Buch wird in den folgenden Kapiteln zunächst in die technischen und rechtlichen Grundlagen der Nutzung und der Überwachung von E-Mail in der Bundesrepublik eingegangen, bevor die Installation und Nutzung der obigen Programme beschrieben wird. Der Einstieg in die Nutzung der Programme soll mit diesem Buch so einfach wie möglich gemacht werden.

E-Mail: Grundlagen, rechtliche Situation und das Prinzip der Verschlüsselung

Grundlagen

Die Kommunikation per E-Mail gehört seit den Anfängen des Internet zu den populärsten Anwendungen. Einfachheit und Schnelligkeit sind die wesentlichen Gründe, warum die E-Mail derart populär wurde. Eine E-Mail ist eine einfache Datei, die aus zwei Teilen besteht, dem

- Header, der alle Stationen der E-Mail auf dem Weg zum Empfänger, den Absender, den Empfänger, das Datum der Erstellung sowie das Format des Inhalts definiert und dem
- Body, den eigentlichen Inhalt der E-Mail, bestehend aus Text und gegebenenfalls Anhängen.

Der Quelltext einer E-Mail sieht beispielsweise so aus:

Return-Path:
Delivered-To: info@dsb-baden-baden.de
Received: from [192.168.1.21] (ip-xxx-xxx-xxx-xxx.unitymediagroup.de [xxx.xxx.xxx.xxx])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(Client did not present a certificate)
by mail.endesha.de (Postfix) with ESMTPSA id 742771FC076
for ; Fri, 19 Jul 2013 12:23:00 +0200 (CEST)
Message-ID: 51E91382.7000906@mein-baden-baden.de>
Date: Fri, 19 Jul 2013 12:22:58 +0200
From: Peter Dippold
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:17.0) Gecko/20130623 Thunderbird/17.0.7
MIME-Version: 1.0
To: info@dsb-baden-baden.de
Subject: Test - =?ISO-8859-15?Q?unverschl=FCsselt?=
X-Enigmail-Version: 1.5.1
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit

Dies ist ein Test

--
Datenschutzbeauftragter (IHK)

Peter Dippold
Eichelgartenstr. 6
76530 Baden-Baden

Die Details im Header bleiben den meisten Usern verborgen, da die Mailprogramme zum Zweck der besseren Lesbarkeit diese in der Standardansicht auf Basisinformationen reduzieren. Dennoch sollte an

dieser Stelle fest gehalten werden, dass die Informationen im Header durchaus auch Informationen enthalten können, die beispielsweise für polizeiliche Ermittler und andere Dritte interessant sein können.

Der Inhalt einer Mail wird im Body entweder im HTML-Format, im Quelltext nicht ganz so leicht lesbar wie unsere Testmail, oder aber als reine Text-Mail dargestellt, letzteres hängt von den Einstellungen im Mailprogramm ab. Dateianhänge, wie beispielsweise Fotos oder Grafiken, werden binär versandt.

Vereinfacht dargestellt, läuft der Versand und Empfang einer E-Mail wie folgt ab:
Versendet ein User A eine Mail an User B, wird die Mail zunächst an den Mailserver des Internet-Service-Providers des Users A übermittelt. Der Mailserver des Users A schickt seinerseits die Mail über möglicherweise mehrere Stationen an den Mailserver des Internet-Service-Providers des Users B, der wiederum die Mail zur Abholung für User B bereit hält. Da die allermeisten Mails im Klartext versandt werden, ist es an allen Punkten des Weges immer möglich, die Mail zu lesen, Kopien anzufertigen und, im Extremfall, sogar zu verändern, ohne dass der Empfänger dies bemerkt. Ist die Mail auf dem Mailserver des Providers des Users B angekommen, kann der Empfänger diese entweder über das Post Office Protocol (POP3) oder aber über das Internet Message Access Protocol (IMAP) abrufen. Verwendet er das IMAP Protokoll verbleiben die Mails auf dem Mailserver und können durch verschiedene Endgeräte, PC, Smartphone, Notebook gleichermaßen gelesen und bearbeitet werden. Im Fall der Nutzung von POP3 entscheidet der User selbst, ob eine Kopie auf dem Server verbleibt. Im Falle eines Verlusts des heimischen Rechners sind die Mails, sofern keine Sicherungskopien angelegt und POP3 ohne Sicherungskopie auf dem Mailserver genutzt wurde, verloren.

Die unverschlüsselte E-Mail kann also durchaus mit der offenen Postkarte verglichen werden, die üblicherweise von Dritten, die Zugang zu den betreffenden Mailservern (oder Knotenpunkten des Internet) haben, mit gelesen werden können. Die verwendeten Mailserver können, müssen aber keineswegs im Heimatland der Empfänger stehen, was dazu führt, dass unterschiedliche internationale Rechtssysteme und Mentalitäten betroffen sein können. Um so erstaunlicher, dass immer wieder selbst im kritischen Geschäftsverkehr vertrauliche Informationen, "geschützt" durch einen in der Praxis unwirksamen Disclaimer, offen und unverschlüsselt versandt werden.

Rechtliche Grundlagen in Deutschland und praktische Umsetzung

In Deutschland wird der Zugriff Dritter auf E-Mails sowie internetbasierte Kommunikation in der Telekommunikations-Überwachungsverordnung (TKÜV) und im Telekommunikationsgesetz (TKG) geregelt. Internet-Service-Provider, die mehr als 10.000 Konten verwalten, müssen entsprechend der TKÜV und §110ff TKG technische Vorrichtungen vorhalten, die sogenannte SINA-Box, die es berechtigten Stellen erlauben, direkt auf den Mailverkehr der Kunden des Providers zuzugreifen und Kundenmails über eine VPN Verbindung an die Polizei, den Zoll, Bundes- oder Landesminister sowie die verschiedenen Verfassungsschutzämter der Länder und des Bundes übermitteln. Die Kosten für die Implementierung der Überwachungseinrichtung und den laufenden Betrieb hat der Provider zu übernehmen. Der Bundesnachrichtendienst führt ferner eine sogenannte strategische Überwachung durch, mit der gezielt nach Stichwörten zur Terrorismusbekämpfung, zur Bekämpfung von Schleuserdiensten sowie zum Bereich Proliferation und konventionelle Rüstung durchsucht werden. Soweit bislang qualifizierte Informationen über das amerikanische PRISM-Programm vorliegen, wurden die Metadaten der Kommunikation, vermutlich E-Mail Header, gespeichert und ausgewertet. Für eine sachliche Bewertung ist es sicher zu früh, es fehlen qualifizierte Informationen darüber, wer die Speicherung und den Zugriff anordnete und kontrollierte, in wie weit rechtsstaatlich übliche Grundsätze eingehalten oder gebrochen wurden. Und es fehlen qualifizierte Informationen darüber, ob und wie weitgehend Prism tatsächlich Anschläge und Terroraktionen verhindert hat. Die Einschätzung nach der Verhältnismäßigkeit der Mittel steht in diesem Fall aus. Die Internationalität des Vorgangs

macht aber auch deutlich, dass der Schutz der Privatsphäre keineswegs eine nationale Angelegenheit alleine mehr sein kann. Aufklärung und, im ersten Schritt leichter umsetzbar, individuelle Schutzmaßnahmen stehen auf der Tagesordnung.

Das Prinzip der asymmetrischen Verschlüsselung

Unsere Grafik 1 zeigt exemplarisch, nach welchem Prinzip der Schutz ihrer individuellen Kommunikation per E-Mail möglich ist:

Grafik 1: Das Prinzip der Verschlüsselung

Wie in der Grafik dargestellt, werden generell zwei verschiedene Schlüssel benötigt, der öffentliche und der private Schlüssel des Inhabers. Den öffentlichen Schlüssel stellt der Besitzer des Mailpostfachs allen zur Verfügung, die mit ihm geschützt kommunizieren möchten. Dazu bieten sich mehrere Möglichkeiten an, der Besitzer des öffentlichen Schlüssels

- kann diesen, wie in der Grafik gezeigt, per Mail an Interessenten senden oder er
- kann einen Schlüsselserver-Dienst nutzen und allen Internetnutzern damit zugänglich machen oder er
- kann diesen zum Download auf seiner eigenen Website anbieten.

Der private Schlüssel darf keinesfalls in die Hände Dritter gelangen. Der Verlust des privaten Schlüssels oder aber, auch das passiert bei längere Zeit nicht mehr genutzten Schlüsseln, der Passphrase, führt automatisch dazu, dass sich Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, nicht mehr entschlüsseln lassen und somit auch für den Empfänger unlesbar bleiben. Es kommt also darauf an, ein adäquates Schlüsselmanagement mit Sicherungskopien zu entwickeln, um derartige Fehlentwicklungen zu vermeiden.

Darüber hinaus besteht die Möglichkeit, ein sogenanntes Widerrufszertifikat zu erzeugen, mit dem die Rücknahme eines über Schlüsselserver-Dienste veröffentlichten Schlüssel möglich ist, Details auch hierzu in den folgenden Kapiteln.

Eine gewichtige Einschränkung ist an dieser Stelle bereits angebracht: Wie eingangs dargelegt, besteht eine Mail aus zwei Teilen, dem Header und dem Body mit dem eigentlichen Inhalt. Damit ein Maildienst überhaupt funktionieren kann, darf der Header auf keinen Fall verschlüsselt werden. Hier bleiben also sämtliche Informationen frei lesbar, wie sonst sollte die Zustellung an den gewünschten Empfänger auch funktionieren, wenn dieser nicht im Klartext lesbar wäre. Sofern sich also Überwachungsmaßnahmen auf den Bereich des Headers konzentrieren, beispielsweise um Kommunikationsstrukturen transparent zu machen, ist Verschlüsselung keine geeignete Maßnahme, das zu unterbinden. Hier versagt der Selbstschutz.

Für den Schutz des Inhalts einer E-Mail gibt es aus meiner Sicht aktuell keine Alternative. Eine verschlüsselte E-Mail kann selbst bei dauerhafter Speicherung auf dem Mailserver, beispielsweise bei Nutzung von IMAP, von niemandem gelesen werden, der nicht im Besitz des privaten Schlüssels ist. Ermittlungsbehörden, die neben den Daten des Headers auch auf Inhalte zugreifen wollen, müssen hier auf die E-Mail entweder beim Absender vor dem Verschlüsseln oder beim Empfänger nach dem Entschlüsseln zugreifen, was nur durch den Einsatz von Trojanern auf dem Rechner des Empfängers oder des Absenders möglich ist.

Installation

2.1. Installation unter Windows (Linux User wechseln gleich zum Abschnitt 2.2)

Zunächst benötigen Sie einen Mailclient, ich möchte Ihnen hier den Thunderbird-Mailclient des Mozilla-Projekts, das auch den in Deutschland beliebten Firefox Webbrowser verantwortet, empfehlen. Sie erhalten Thunderbird unter der Adresse

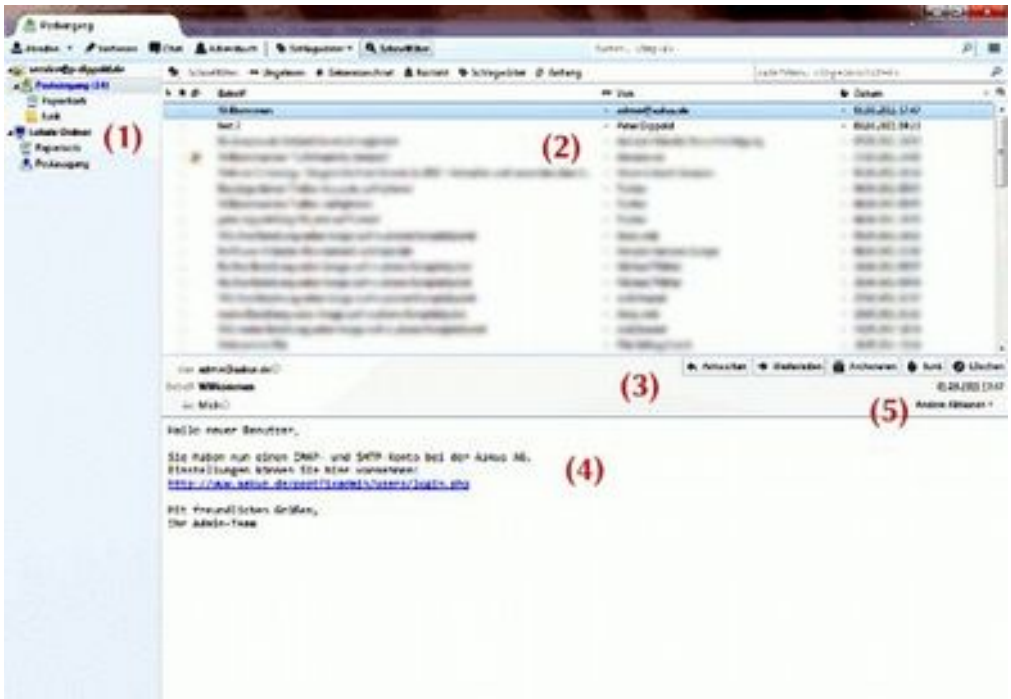
https://www.thunderbird-mail.de/herunterladen/

Die aktuelle Version 52.9.1 für Windows läuft auch auf 64-Bit-Systemen. Laden Sie die .exe-Datei auf Ihren Rechner und folgen Sie einfach dem Installationsassistenten.

Nachdem die Installation erfolgreich abgeschlossen und Thunderbird gestartet wurde, können Sie entweder eine neue Mailadresse beantragen oder aber Ihr bestehendes Mailkonto anlegen. Die benötigten Daten hierfür haben Sie vom Mailprovider erhalten. Bei großen Mailprovidern, wie beispielsweise Google, reicht die Eingabe des Benutzernamens und des Passworts aus, Thunderbird findet die restlichen Einstellungen automatisch. Mitunter ist es jedoch erforderlich, die benötigten Daten im zweiten Schritt von Hand manuell nach zu pflegen.

Nachdem Sie Ihr erstes Mailkonto angelegt haben, präsentiert sich die Thunderbird-Oberfläche so:

Grafik 2: Die Thunderbird-Oberfläche



Unter (1) finden Sie auf der linken Seite Ihre Mailkonten, Thunderbird kann mehrere Mailkonten verwalten. Das Anlegen neuer Mailkonten realisieren Sie über den Menübefehl ***Datei**Neu**Existierendes Mailkonto*. Unter (2) finden Sie die Kennzeichnung Ihrer Mails, die im Fensterbereich unter (3) angezeigt werden. Funktionen wie "Antworten", "Weiterleiten",

"Archivieren", "Junk" und "Löschen oberhalb des Fensterbereichs mit dem Mailinhalt, unter (5), "Andere Aktionen" können Sie sich unter anderem auch den Quelltext einer Mail anzeigen lassen.

Mit dem erfolgreichen Installieren und Einrichten von Thunderbird haben Sie den ersten Schritt zur geschützten Kommunikation per E-Mail bereits erfolgreich bewältigt.

Nun benötigen Sie im nächsten Schritt das Open Source Programm GnuPG, für Windows ist unter

https://www.gpg4win.org/download-de.html

eine komplette Installationssuite inklusive GnuPG in der aktuellen Version 3.1.2 enthalten. Auch hier ist die Installation mit Hilfe der .exe Datei einfach, Sie sollten sich aber unbedingt Papier und einen Stift zurechtlegen, um den Pfad, in den GnuPG installiert wird, zu notieren, da Enigmail aktuell diesen nicht automatisch findet. Unter Windows 7 lautete in der Standardversion der Pfad

C:\Programme (x86)\GNU\GnuPG\gpg2.exe

Unter Windows 10 C:\Programme(x86)\GnuPG\bin\gpg.exe

Auch diese Installation ist rasch und einfach erledigt.

Ein wenig trickreicher, aber auch nicht unüberwindbar, gestaltet sich der nächste Schritt. Nun installieren Sie über Thunderbird das Add-on Enigmail. Die aktuelle Version ist 2.0.7 und wird über den Add-on Manager von Thunderbird installiert. Hierzu rufen Sie im Menue unter ***Extras**Add-ons* den Add-on Manager auf und geben im Suchfeld oben rechts den Suchbegriff "Enigmail" ein. Mit Klick auf "Installieren" starten Sie die Installation, die bis auf einen Schritt, automatisch abläuft. Im Verlauf der Installation teilt Ihnen der Installationsmanager mit, dass er keine installierte Version von GnuPG finden konnte und bietet Ihnen die Möglichkeit der manuellen Suche. Gut, wenn Sie sich bei der Installation von gpg4win den Pfad aufgeschrieben haben. Sollte das nicht geschehen sein, suchen Sie einfach über die Suche nach der Datei gpg2.exe. Diese Datei wählen Sie aus und Enigmail wird komplett und einwandfrei installiert.

Windows User können den folgenden Linux Teil überspringen und direkt zur Einrichtung von Enigmail im Abschnitt 2.3. übergehen.

2.2. Installation unter Linux (Ubuntu)

Die Installation unter Linux, hier die aktuelle Ubuntu LTS Version, gestaltet sich unproblematisch. Sofern noch nicht installiert, das sollte eigentlich schon mit der Basisinstallation des Systems geschehen sein, installieren Sie Thunderbird mit dem Befehl

sudo apt-get install thunderbird

Beim ersten Start von Thunderbird werden Sie aufgefordert, ein aktuelles E-Mailkonto anzulegen, hier geben Sie entweder die Daten Ihres E-Mailkontos ein, oder bestellen einfach eine neue Mailadresse.

Die Installation von GnuPG erledigen Sie mit

sudo apt-get install gnupg

Hier sind weitere Schritte nicht mehr erforderlich, da Sie die Zertifikatsverwaltung komfortabel über Enigmail realisieren können.

Enigmail installieren Sie nun über den Add-on Manager von Thunderbird. Wählen Sie hierzu im Menü von Thunderbird **Extras**Add-ons* und geben rechts oben im Suchfeld "Enigmail" ein. Mit Klick auf "Installieren" wird Enigmail Thunderbird hinzu gefügt. Standardmäßig wurde GnuPG als gpg im Verzeichnis /usr/bin/ installiert, normalerweise findet das Installationsprogramm von Enigmail GnuPG, sollte dies einmal nicht der Fall sein, werden Sie nach dem korrekten Pfad der GnuPG Installation gefragt.

2.3. Abschließende Einrichtung von Enigmail mit dem GnuPG Assistenten unter Windows und Linux

Nachdem Enigmail sauber installiert wurde, finden Sie im Menü von Thunderbird einen neuen Menüpunkt Enigmail. Um Ihren ersten Schlüssel zu erstellen bieten sich zwei verschiedene Wege an. Entweder nutzen Sie den Einrichtungsassistenten, der erste Submenüpunkt unter Enigmail, oder Sie wechseln gleich zur Schlüsselverwaltung. Die ersten Schritte gehen Sie vielleicht besser mit dem Einrichtungsassistenten. Bestätigen Sie im ersten Schritt, dass Sie sich vom Assistenten helfen lassen möchten. Im nächsten Schritte wählen Sie aus, für welches Konto Sie ein Zertifikat erstellen möchten.

Wenn Sie den Assistenten zum ersten Mal benutzen, werden Sie nun aufgefordert, ein neues Schlüsselpaar zu erzeugen, im Wiederholungsfall können Sie wählen, ob Sie einen vorhandenen Schlüssel nutzen möchten, oder aber ein neues Schlüsselpaar erzeugen möchten. Wenn Sie ein neues Schlüsselpaar erzeugen, werden Sie im nächsten Schritt nach einer Passphrase gefragt.

Wählen Sie hier eine sichere Passphrase, die Sie sich zudem gut merken können.

Wichtiger Hinweis:
Geht die Passphrase verloren, ist der Schlüssel unbrauchbar. Deshalb sollten Sie diesen Schritt mit größtmöglicher Sorgfalt ausführen. Eine gute Möglichkeit, ein sicheres Passwort zu erstellen ist der Gebrauch eines einfachen, leicht zu merkenden Satzes, zum Beispiel "Ich bin Vorname und Nachname und habe am 11.11.1975 meine heutige Frau geheiratet" - aus den Anfangsbuchstaben und Zahlen generieren Sie in diesem Beispiel das Passwort "IbVuNuha11.11.1975mhFg". Sie sollten für ein ausreichendes Maß an Sicherheit den Passwortsatz nicht zu kurz wählen.

Klicken Sie nun auf weiter und erzeugen Sie Ihren Schlüsselsatz, bestehend aus privatem und öffentlichem Schlüssel.

Abschließend werden Sie, sofern die Generierung der Schlüssel erfolgreich war, gefragt, ob Sie ein Widerrufszertifikat erstellen möchten. Wir empfehlen dringend, diesen Schritt nicht zu überspringen und das Widerrufszertifikat auf Ihrem Rechner zu speichern. Mit Hilfe des Widerrufszertifikats können Sie Ihren Schlüssel bei Missbrauch oder Verlust zurückziehen.

Einstellungen in Enigmail und Thunderbird

Nach der erfolgreichen Installation von Enigmail finden Sie im Menü von Thunderbird den neuen Menüpunkt "Enigmail". Wahrscheinlich haben Sie bereits bei der Erstimplementierung einen Schlüsselbund bestehend aus privatem und öffentlichem Schlüssel angelegt. Falls Sie dies versäumt haben sollten, lesen Sie bitte zunächst das Kapitel zur Schlüsselverwaltung, bevor Sie hier weiter fortfahren.

In der Regel haben Sie bereits ein Schlüsselpaar erstellt und sollten nun einige Einstellungen vornehmen, die Ihnen die künftige Arbeit mit Ihrem Verschlüsselungssystem erleichtern. Zunächst wählen Sie im Menü von Thunderbird ***Enigmail**Einstellungen* und aktivieren mit Klick auf die entsprechende Schaltfläche die "Experten-Optionen". Die Zahl der Reiter der Einstellung hat sich nun deutlich erhöht und Sie können neben den Basics eine ganze Reihe fortgeschrittener Einstellungen vornehmen.

Zunächst können Sie die Ablaufzeit der Passphrase in den Einstellungen ändern, die Vorgabe von fünf Minuten ist etwas zu kurz, hier können Sie gerne einen deutlich längeren Wert wählen. Die Abfrage der Passphrase durch Anklicken von "Nie nach einer Passphrase fragen" empfiehlt sich nicht. Im oberen Bereich der Einstellungen unter "Allgemein" finden Sie den Pfad zum Programm GnuPG, hier müssen Sie unter Windows wie im Installationskapitel beschrieben gegebenenfalls eine Änderung vornehmen.

Im Reiter "Senden" sollten Sie keine Änderungen des Standards vornehmen, die zusätzliche Verschlüsselung mit dem eigenen Schlüssel ermöglicht Ihnen versandte Mails im "Gesendet"-Verzeichnis zu lesen. Sollten Sie ein Fan leerer Betreffzeilen sein, müssen Sie zusätzlich die Option "Leere Betreffzeile erlauben" aktivieren.

Im Reiter "Schlüsselauswahl" ist die Option "Durch Empfängerregeln oder E-Mail-Adressen" voreingestellt. Alternativ können Sie hier wählen, ob Sie nur durch Empfängerregeln, nur durch E-Mail-Adressen oder manuell den Schlüssel zum Versenden von E-Mails auswählen möchten. Die Option "Keine manuelle Auswahl der Schlüssel" verhindert, dass Enigmail nach dem Schlüssel fragt, wenn weder die E-Mail-Adresse, noch eine Empfängerregel zugeordnet werden können. Ist diese Option nicht aktiviert fragt Enigmail andernfalls, welcher Schlüssel für den Versand einer Mail zugeordnet werden soll. Wenn Sie sich nicht sicher sind, welche Einstellung für Sie die passende ist, sollten Sie es zunächst bei der Vorauswahl "Durch Empfängerregeln oder E-Mail-Adressen" belassen und, für den Fall von Komplikationen eventuell die Einstellung "Manuell" prüfen. Ist die letztere Option eingestellt, fragt Enigmail immer, welcher Schlüssel für den Versand einer zu verschlüsselnden Mail gewählt werden soll.

Im Reiter "Erweitert" sollten Sie die voreingestellten Optionen belassen, lediglich die voreingestellte Option "Anhänge nur herunterladen, wenn diese geöffnet werden sollen (nur bei IMAP)" sollten Sie, sofern Sie IMAP benutzen, deaktivieren. Mit dieser Änderung stellen Sie sicher, dass Nachrichten, die größer als 40 KB sind, korrekt entschlüsselt werden. Ist diese Option aktiviert, kann es zu Konflikten kommen, da Thunderbird Anhänge erst bei Aufruf lädt und so bei größeren Texten der E-Mail nicht erkennt, dass es sich hier nicht um einen Anhang handelt.

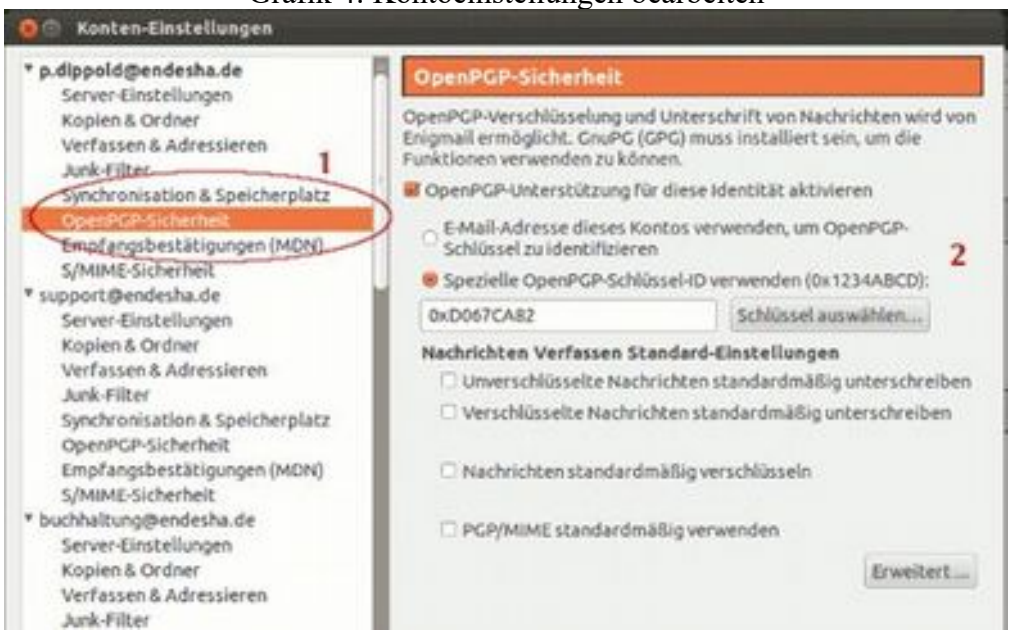
Die voreingestellten Schlüsselserver unter dem Reiter "Schlüssel-Server" sollten Sie unverändert belassen.

Sollte es zu Konflikten in der Zusammenarbeit zwischen Thunderbird und Enigmail kommen, sind die Einstellungen im Reiter "Fehlersuche" hilfreich. Zum einen können Sie hier einen Ordner für Log-

Dateien angeben, zum anderen können Sie darunter die Zusammenarbeit von Enigmail und Thunderbird direkt testen. Geben Sie hier einfach Ihre Mailadresse ein und klicken auf Testen.

Möglicherweise verwalten Sie mit Thunderbird und Enigmail mehrere Konten mit unterschiedlichen Schlüssel beispielsweise um private Mails und geschäftliche zu trennen, dann sollten Sie nach erfolgreicher Installation von Enigmail und Thunderbird, einschließlich Schlüsselerzeugung, sich den Bereich der Thunderbird-Konten ansehen. Hierzu klicken Sie auf den Kontonamen oberhalb des Posteingangs und anschließend auf "Konten-Einstellungen bearbeiten".

Grafik 4: Kontoeinstellungen bearbeiten



Klicken Sie bei den Konteneinstellungen für das betreffende Konto links auf "OpenPGP-Sicherheit"(1).
Sollten Sie mehrere Mailadressen und unterschiedliche Konten verwalten, können Sie hier festlegen, ob Sie zur Identifikation des passenden Schlüssels die E-Mailadresse verwenden, oder aber, ob Sie mit Klick auf "Schlüssel auswählen" einen speziellen Schlüssel definieren möchten (2). Sollte es mehrere Schlüssel geben, werden Sie im ersten Fall gefragt welcher Schlüssel zur Entschlüsselung gewählt werden soll. Die Optionen unter "Nachrichten Verfassen Standard-Einstellungen" werden, sofern Empfängerregeln definiert sind, ignoriert. Mit Klick auf "Erweitert" können Sie Nachrichtenempfängern Hilfestellungen zum Erhalt Ihres öffentlichen Schlüssels geben.

Schlüsselverwaltung und Empfängerregeln

Sie hatten bereits bei der Installation von Enigmail vermutlich Ihren ersten Schlüssel erzeugt. Sollten Sie diesen Schritt übersprungen haben, können Sie dies nun nachholen. Oder Sie benötigen für ein weiteres Mailkonto einen zweiten Schlüssel, beispielsweise um geschäftliche und private Post mit unterschiedlichen Schlüsseln zu versehen. Die Erzeugung eines neuen Schlüsselpaares, bestehend aus öffentlichem und privaten Schlüssel ist einfach.

Die Schlüsselverwaltung in Enigmail erreichen Sie im Thunderbird Menü mit ***Enigmail**Schlüssel verwalten*.

Im sich öffnenden Fenster erhalten Sie eine Übersicht, über alle bislang selbst erzeugten und von Dritten erhaltenen öffentlichen Schlüssel. Möglicherweise ist diese Liste noch kurz geraten. Mit der Zeit wird sich die Liste deutlich verlängern und die Zahl Ihrer Kontakte, die eine geschützte Kommunikation vorziehen, hoffentlich zunehmen. Im Suchfeld können Sie gezielt nach einem bestimmten Schlüssel, den Sie bereits erhalten haben, suchen. Zum Erzeugen eines neuen Schlüsselpaares, bestehend aus öffentlichem und privatem Schlüssel, klicken Sie im Menü der Schlüsselverwaltung auf ***Erzeugen**neues Schlüsselpaa*r. Im darauf folgenden Dialog wählen Sie unter Benutzer-ID die Mailadresse, für die das Schlüsselpaar erzeugt werden soll und klicken auf "Schüssel zum Unterschreiben verwenden", wenn dies in den OpenPGP Optionen des oben ausgewählten Mailkontos eingetragen werden soll.

Unter Passphrase tragen Sie ein sicheres, gut zu merkendes Passwort ein, wie man ein solches erzeugt, haben wir im Kapitel über die Installation bereits beschrieben. Die Passphrase muss im zweiten Feld wiederholt werden. Einen Schlüssel ohne Passphrase zu erzeugen, auch diese Möglichkeit bietet sich hier, ist keine gute Idee. Das Kommentarfeld ist optional. Das Ablaufdatum des Schlüssels geben Sie darunter ein, soll der Schlüssel unbegrenzt gültig sein, haken Sie die daneben befindliche Checkbox an. Über den Tab "Erweitert" können Sie zudem die Schlüsselstärke bestimmen, es empfiehlt sich hier, es bei den Standardwerten zu belassen.

Hinweis: Falls Sie neben der privaten Kommunikation eine oder mehrere geschäftliche Adressen verwalten, die unter Umständen sogar mit mehreren Mitarbeitern geteilt werden, empfiehlt es sich, ein Schlüsselpaar für den privaten, ein weiteres für den geschäftlichen Gebrauch, mit jeweils unterschiedlichen Passphrasen zu erzeugen. Der Einsatz betrieblicher Schlüssel wird in der Regel durch die Geschäftsleitung und/oder die damit betrauten Administratoren angeordnet und realisiert.

Mit Klick auf "Schlüsselpaar erzeugen" haben Sie nun erfolgreich Ihren ersten oder zweiten Schlüssel erzeugt. Im nächsten Schritt macht es Sinn, zu Ihrem nun erzeugten Schlüssel ein Widerrufszertifikat zu erzeugen. Mit Hilfe des Widerrufszertifikats können Sie Ihren öffentlichen Schlüssel, wenn Sie diesen auf einen öffentlich zugänglichen Schlüsselserver geladen haben, zurücknehmen. Dies ist notwendig, wenn Sie ihren privaten Schlüssel verlieren, beispielsweise bei einem Festplattenschaden, ohne dass Sie über eine Sicherungskopie verfügen oder aber wenn Sie Ihre Passphrase verlegt oder vergessen haben, was bei längere Zeit nicht genutzten Schlüsseln auch vorkommen kann.

Zum Erzeugen eines Widerrufszertifikats wählen Sie, sofern nicht ohnehin schon geöffnet, im Thunderbird-Menü erneut mit ***OpenPGP**Schlüssel verwalten* die Schlüsselverwaltung aus und markieren im geöffneten Fenstern den Schlüssel, für den Sie das Widerrufszertifikat erzeugen möchten. Anschließend wählen Sie im Menü der Schlüsselverwaltung ***Erzeugen**Widerrufszertifikat* aus. Im sich öffnenden Dialog können Sie ein Widerrufszertifikat in Form einer ASCII-Datei mit der Dateiendung .asc erzeugen, wählen Sie hier einen ausdrucksstarken Klarnamen für Ihr Zertifikat, der ihnen erleichtert, auch zu einem späteren Zeitpunkt die Funktion des Zertifikats noch wiedererkennen zu können.

Wo befinden sich nun Ihre Schlüssel auf dem Rechner?

Unter Linux finden Sie die erzeugten Schlüssel in der Regel in Ihrem Heimverzeichnis unter .gnupg. Im Verzeichnis finden Sie eine eine pubring.pgp und eine secring.pgp, die beiden Binärdateien enthalten alle bereits angelegten bzw. importierten Schlüssel. Diese binären Dateien sind für den Versand an Dritte nicht geeignet.

Unter Windows finden Sie in der Regel diese Dateien unter C:\Users\Username\AppData\Roaming\gnupg

Den öffentlichen Schlüssel verteilen

Ihren öffentlichen Schlüssel, möglicherweise haben Sie für unterschiedliche Mailkonten auch mehrere, können Sie auf mehreren Wegen verteilen:

- per E-Mail direkt an einen Ihrer Kontakte
- als ASCII-Datei auf Ihrer Homepage oder Ihrem Block hinterlegen oder
- auf einen öffentlichen Schlüsselserver laden.

Den Versand Ihres öffentlichen Schlüssels per E-Mail können Sie entweder direkt aus dem Programm "Schlüsselverwaltung" realisieren, indem Sie Ihren Schlüssel markieren und im Menü der Schlüsselverwaltung unter ***Datei**öffentlichen Schlüssel versenden* anklicken. Dieser Befehl erzeugt eine neue E-Mail mit dem angehängten Schlüssel im ASCII-Format mit der Endung .asc. Ihr privater Schlüssel wird bei Nutzung dieser Option selbstverständlich nicht mit gesendet.

Der Quelltext der generierten Mail könnte beispielsweise so aussehen:

Message-ID: 51EB957E.9010502@dsb-baden-baden.de>
Date: Sun, 21 Jul 2013 10:02:06 +0200
From: Peter Dippold
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:17.0) Gecko/20130623 Thunderbird/17.0.7
MIME-Version: 1.0
To: autor@p-dippold.de
Subject: Oeffentlicher Schluessel
X-Enigmail-Version: 1.5.1
Content-Type: multipart/mixed;
boundary="------------030009020904070608030202"

This is a multi-part message in MIME format.
--------------030009020904070608030202
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit

Hallo,
anbei mein öffentlicher Schluessel.
Gruß
Peter

--

Datenschutzbeauftragter (IHK)
Peter Dippold
Eichelgartenstr. 6
76530 Baden-Baden

--------------030009020904070608030202
Content-Type: application/pgp-keys;
name="0xD067CA82.asc"
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
filename="0xD067CA82.asc"

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBFHVLWsBCADM/57SLijajn5gTmZlBVitgRp46ezHXuZSOCzX6c3UOquKBQTz
dUNoEOIuFTcOWfbKqkZcnfZbqzSO00QnGPD1CyEdJLsKUqIXfEiE3q8CZI5h3Iup
rk4s+/qDmWX8ffZ6kp9fMEOCrIuk4iFyjoPXNOnZvZ7pEe22ZFBWAso6QwTq2gtw
...
JCy4Xa14yyRwHM4OlbnpsjU4iOhr5fdjqN4RlsJWQTZz6Y2Xi19/G0dcaYhfwqyK
LWrUW+MY6DKkXHKO6nGO26zRxmTv6RUc9nP+/RLBwT/EeLYXlzlPTePtArc17nw=
=s/VB
-----END PGP PUBLIC KEY BLOCK-----

--------------030009020904070608030202--

Aus Gründen der Lesbarkeit wurde der erste Teil der Mail nicht verschlüsselt. Gut zu erkennen ist die Textdatei des Schlüssels im Quelltext der Mail (Ausschnitt), die beim Empfänger direkt in den Schlüsselbund per Mausklick integriert und genutzt werden kann.

Alternativ zu dieser Variante können Sie ihren öffentlichen Schlüssel zunächst auch per Exportfunktion in Enigmail als ASCII-Datei auf Ihrem Rechner abspeichern und anschließend in einer E-Mail als Anhang versenden. Hierzu wählen Sie im Menü der Schlüsselverwaltung ***Datei**Exportieren*, nachdem Sie zuvor den zu exportierenden Schlüssel markiert hatten. Nun exportieren Sie den markierten Schlüssel auf einen beliebigen Platz auf Ihrer Festplatte. Sie können auf diese Weise eine Sicherungskopie aller erhaltenen Schlüssel, auch der öffentlichen Schlüssel Dritter auf Ihrem Rechner sichern. Als Besitzer mindestens eines Schlüsselpaares, bestehend aus öffentlichem und privatem Schlüssel, können Sie das Schlüsselpaar auf gleichem Weg auf der Festplatte im ASCII Format sichern. Wollen Sie nur den öffentlichen Schlüssel Ihres eigenen Schlüsselpaares sichern, wählen Sie die entsprechende Option im Dialog aus.

Hinweis: Wenn Sie eine Sicherungskopie Ihres öffentlichen und des privaten Schlüssels anfertigen, eine sinnvolle Maßnahme um einem Schlüsselverlust vorzubeugen, sollten Sie auf eine eindeutige Dateibezeichnung achten, um möglichen Interessenten an Ihrem öffentlichen Schlüssel nicht versehentlich beide Schlüssel als Dateianhang zu senden.

Falls Sie über einen eigenen Blog, eine Website oder einen Onlineshop verfügen, können Sie Ihren öffentlichen Schlüssel natürlich auf hier zum Download im exportierten ASCII-Format anbieten.

Eine dritte Möglichkeit, Ihren öffentlichen Schlüssel zu verbreiten, können Sie im Menü der Schlüsselverwaltung mit Klick auf ***Schlüssel-Server**Schlüssel hoch laden* rasch realisieren, nachdem Sie zuvor einen oder mehrere Schlüssel der Schlüsselverwaltung markiert haben. Private Schlüssel werden vom Programm selbstverständlich nicht hoch geladen.

Nachdem Sie nun erfolgreich einen oder mehrere Schlüssel generiert haben, möchten Sie natürlich auch die privaten Schlüssel Ihrer Kontakte erhalten. Als erster Schritt bietet sich hier die Suche über einen der zentralen Schlüssel-Server an. Wählen Sie hier im Menü der Schlüsselverwaltung ***Schlüssel-Server**Schlüssel suchen*. Sie können über eine Ihnen eventuell bekannte Schlüssel-ID oder nach einer bekannten E-Mail Adresse oder Bestandteilen einer E-Mail Adresse suchen. Wenn Sie den gewünschten privaten Schlüssel gefunden haben, markieren Sie die Checkbox links neben den Schlüsselangaben und klicken auf OK, der Schlüssel wird direkt in Ihre Schlüsselverwaltung importiert und steht Ihnen zum Verschlüsseln einer Mail an diese Person zur Verfügung.

Neben der Mailadresse, dem Namen und der Schlüssel-ID wird Ihnen in der Schlüsselsuche auf dem Schlüsselserver auch das Datum der Erstellung angezeigt. Teilweise werden Sie mehrere Jahre alte Schlüssel finden, von denen nicht unbedingt garantiert ist, dass diese noch aktiv im Betrieb des Besitzers sind. Sollte dieser den privaten Schlüssel verloren oder die Passphrase vergessen oder verlegt haben, ist eine Entschlüsselung natürlich nicht mehr möglich. Dies sollten Sie eventuell vorab mit dem Besitzer des Schlüssels klären.

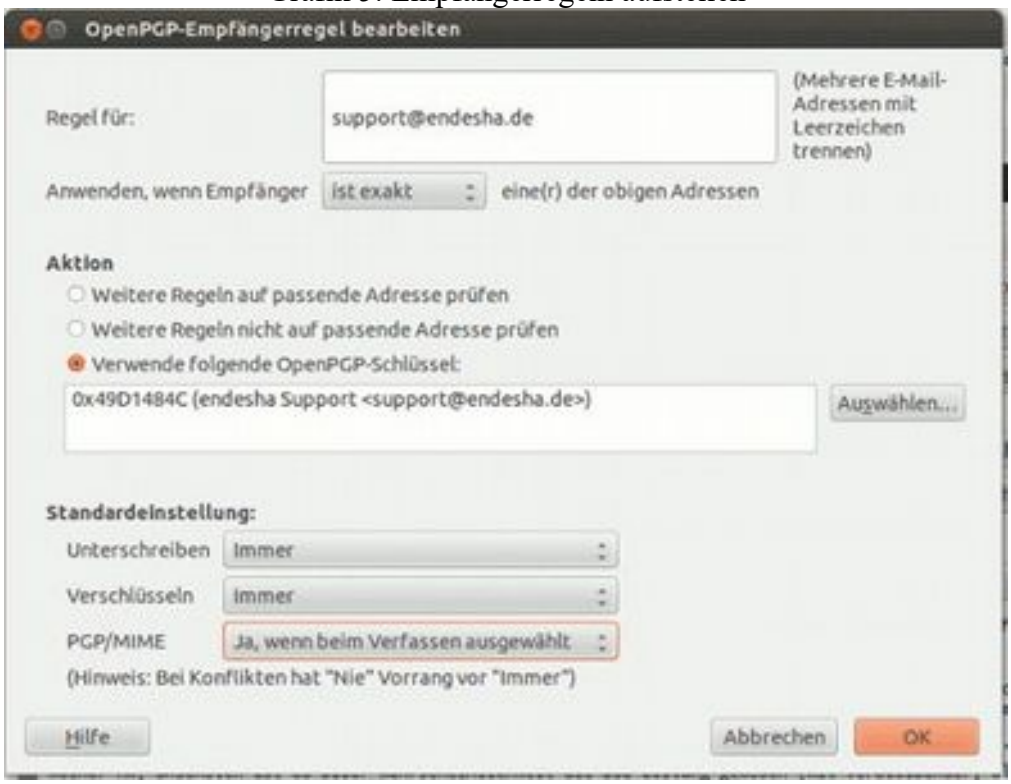
Alternativ steht Ihnen natürlich die Möglichkeit, Ihre Kontakte per Mail um den privaten Schlüssel zu bitten, zur Verfügung. Dieser Weg garantiert Ihnen, dass Sie einen aktiv genutzten Schlüssel erhalten, dessen Besitzer in der Lage ist, ihre verschlüsselten Mails auch zu lesen, was insbesondere bei älteren Schlüsseln auf den öffentlichen Schlüsselservern nicht immer der Fall sein muss.

Empfängerregeln

Sollten Sie für bestimmte Kontakte feste Empfängerregeln festlegen wollen, dann können Sie das mit Enigmail ebenfalls realisieren. Aktivieren Sie hierzu die Experten-Option (***OpenPGP**Einstellungen*), falls nicht ohnehin schon eingestellt und wählen Sie anschließend im Thunderbird-Menü ***OpenPGP**Empfängerregeln*.

Mit "Hinzufügen" können Sie eine neue Empfängerregel aufstellen, wie im Screenshot Beispiel dargestellt:

Grafik 5: Empfängerregeln aufstellen



Empfängerregeln funktionieren natürlich nur, wenn Sie zuvor bei den Einstellungen (***OpenPGP**Einstellungen*) im Reiter Schlüsselauswahl "Durch Empfängerregeln oder E-Mail-Adressen" ausgewählt haben. Sollten hier die Einstellungen auf "Manuell" stehen, macht die Erstellung von Empfängerregeln natürlich keinen Sinn.

Bei den Empfängerregeln können Sie festlegen, ob eine oder mehrere Adressen "Immer", "Gelegentlich" oder "Nie" unterschrieben oder verschlüsselt werden sollen. Auch eine Teilauswahl ist möglich, beispielsweise eine Regel für endesha um alle Mailadressen der endesha AG mit einer Regel zu erreichen.

E-Mails versenden und empfangen

Geschafft - nachdem Thunderbird, Enigmail und GnuPG erfolgreich installiert und eingerichtet, die öffentlichen Schlüssel Ihrer wichtigsten Kontakte besorgt und importiert wurden, können Sie nun daran gehen, Ihre E-Mails sofern gewünscht, einfach und effektiv verschlüsseln. Je nachdem, ob Sie zuvor Empfängerregeln für Ihre Kontakte festgelegt haben, oder aber in den Einstellungen die manuelle Auswahl präferieren, gestaltet sich der Prozess ein wenig unterschiedlich. Ich persönlich ziehe die manuelle Kontrolle einer automatisierten Einstellung vor und möchte von E-Mail zu E-Mail je nach Inhalt und Empfänger unterschiedliche Optionen wählen können. Dies bedeutet an der einen oder anderen Stelle einen Mausklick mehr, erhält Ihnen aber ein Maß an Flexibilität, das mit zunehmender Automatisierung ansonsten verloren geht. Aber das ist Geschmackssache, natürlich können Sie auch andere Einstellungen präferieren und alle Mails an bestimmte Personen oder Institutionen generell unterschreiben und/oder verschlüsseln.

E-Mails verschlüsseln, signieren und senden

Bevor Sie eine Mail versenden, sollten Sie noch eine grundsätzliche Entscheidung darüber treffen, ob Sie bevorzugt Ihre E-Mails als gestaltete und formatierte HTML Mail versenden möchten, oder ob Sie das reine Textformat bevorzugen. Wenn Sie die HTML formatierte E-Mail vorziehen, sollten Sie wissen, dass Sie in diesem Fall als Verschlüsselungsmethode unbedingt PGP/MIME verwenden müssen, da ansonsten Ihre Mail beim Empfänger nicht korrekt angezeigt wird. Die Entscheidung treffen Sie, die Einstellung nehmen Sie für jedes Konto über die Kontoeinstellungen vor. Klicken Sie hierzu auf den Namen des Kontos oberhalb des Posteingangsfaches und anschließend auf der rechten Seite auf "Kontoeinstellungen bearbeiten". Im darauf sich öffnenden Dialog klicken Sie links auf "Verfassen und Adressieren" und wählen entweder rechts oben "Nachrichten im HTML-Format verfassen" oder entfernen den Haken, an dieser Stelle. Unterhalb dieser Auswahlmöglichkeit können Sie die Reihenfolge von Nachricht und Zitat sowie die Reihenfolge einer eventuell eingerichteten Signatur bestimmen. Mit Klick auf OK haben Sie globalen Einstellungen für dieses Konto gesichert.

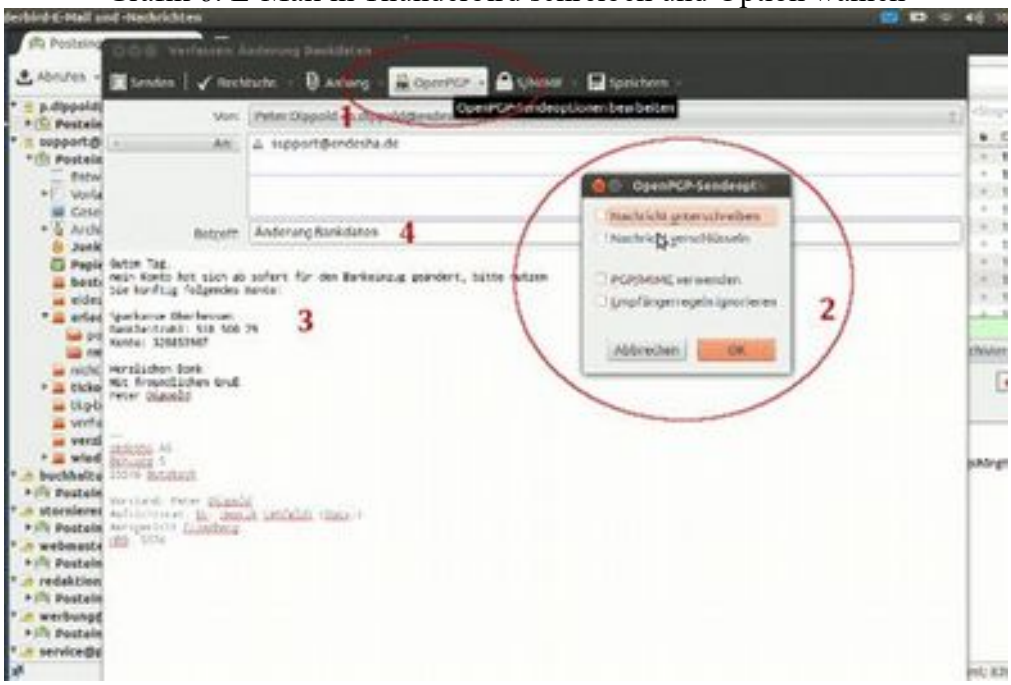
Wie eingangs dieses Buchs beschrieben, benötigen Sie einen gültigen öffentlichen Schlüssel des Empfängers. Um an diesen Empfänger eine Mail zu senden, klicken Sie zunächst auf "Verfassen" oder auch "Antworten" oder "Weiterleiten" in Thunderbird, je nachdem, ob Sie auf eine empfangene Mail antworten, diese weiterleiten oder auch eine neue Mail verfassen möchten.

In den "Einstellungen" zu Enigmail hatten Sie festgelegt, ob Sie die manuelle Schlüsselauswahl oder aber die Auswahl nach Empfängerregel beziehungsweise Mailadresse wünschen. Im vorliegenden Fall wurde die Einstellung auf "Manuell" gesetzt.

Zunächst öffnet sich auf Mausklick das Fenster zum Verfassen oder Weiterleiten einer Nachricht, hier schreiben Sie Klartext.

Im vorliegenden Fall lag der öffentliche Schlüssel des vor, so dass die Entscheidung zugunsten einer Verschlüsselung mit dem öffentlichen Schlüssel und eine Unterzeichnung mit dem eigenen Schlüssel auf der Hand lag. Mit Klick auf ***Enigmail* im Menü (1) öffnet sich die folgende Ansicht:

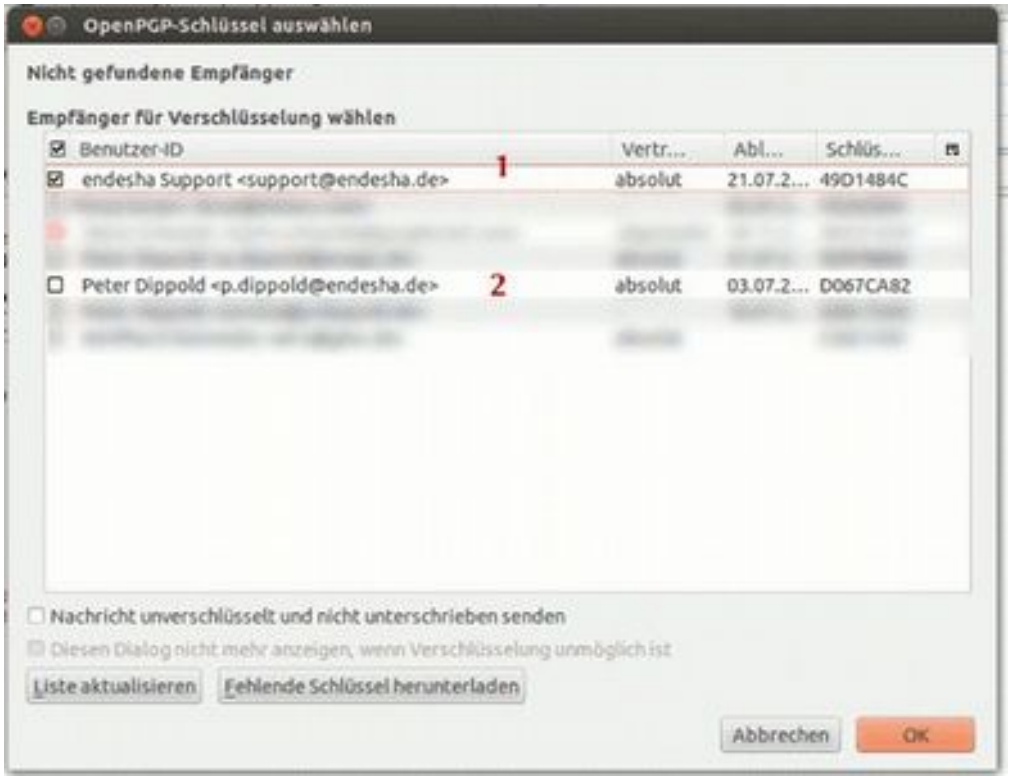
Grafik 6: E-Mail in Thunderbird schreiben und Option wählen



Im Beispiel wurden anschließend die Optionen "Verschlüsseln" und "Signieren" ausgewählt (2), was zur Folge hat, dass der Inhalt der Mail unter (3) mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wurde. Der Text in der Betreffzeile (4) wird dabei nicht verschlüsselt. Die Signatur erfolgt mit dem eigenen Schlüssel, wenn der Empfänger umgekehrt über den öffentlichen Schlüssel des Absenders verfügt, wird zudem auch die Signatur direkt geprüft und das Ergebnis angezeigt.

Da in den Einstellungen die Option "Manuell" gewählt worden war, wird Ihnen nun eine Ansicht der verfügbaren Schlüssel angezeigt und der oder die in Frage kommenden Schlüssel sind bereits gekennzeichnet. Hier können Sie eventuell auch einen alternativen Schlüssel, sofern vorhanden, wählen.
Mit Klick auf Absenden wird die E-Mail sowohl verschlüsselt als auch signiert.

Grafik 7: Wahl des Schlüssels



E-Mails empfangen

Sofern der Empfänger in seinen Einstellungen im Menü unter ***Enigmail* die Option "Automatisch entschlüsseln/überprüfen" gekennzeichnet hat, wird die Mail dem Empfänger im Klartext angezeigt, sofern nicht die Zeit der Gültigkeit der Passphrase abgelaufen ist. Ist letzteres der Fall, wird der Empfänger nach der Passphrase gefragt.

Ein Vergleich der angezeigten Mail mit dem Quelltext der Originalmail zeigt den Unterschied:

Auszug aus der Originalmail:

Guten Tag,
mein Konto hat sich ab sofort für den Bankeinzug geändert, bitte nutzen Sie künftig folgendes Konto:

Sparkasse Oberhessen
Bankleitzahl: 518 500 79
Konto: 328853907

Herzlichen Dank
Mit freundlichem Gruß
Peter Dippold

Und hier die Originalmail, wie Sie auf den Mailservern des Internetservice-Providers zu finden ist und von Dritten gelesen werden kann:

Return-Path:
Delivered-To: info@dsb-baden-baden.de
Received: from [192.168.1.21] (ip-109-91-220-228.unitymediagroup.de [109.91.220.228])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))

(Client did not present a certificate)
by mail.endesha.de (Postfix) with ESMTPSA id BFCAB1FC068
for ; Tue, 23 Jul 2013 17:01:07 +0200 (CEST)
Message-ID: 51EE9AAF.5080907@endesha.de>
Date: Tue, 23 Jul 2013 17:01:03 +0200
From: Peter Dippold
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:17.0) Gecko/20130623 Thunderbird/17.0.7
MIME-Version: 1.0
To: info@dsb-baden-baden.de
Subject: =?ISO-8859-15?Q?=C4nderung_Bankdaten?=
X-Enigmail-Version: 1.5.1
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v1.4.11 (GNU/Linux) Comment: Using GnuPG with Thunderbird -
http://www.enigmail.net/

hQEMA+z+b0pksOyQAQf/RRsB1RtXQIrH0w7vz2Fj0Jyv1jOaSU2niUOCtZavaJ85
DJy5xY56Zs/vPjrFME2M5w8Rf9I0IdcVrS0gIwIcAqJQyV1qZsGb2E7rLuTCOeSA
7RLs+0XBe5sS2/dyKowh5bGutl0e3G0ZlkA5qJB2KZgbgCOJFgA/TQEEw5qLVi1M
...
ud1nlhcvaXlLJV0xJ6SyHusSefH8WdnzbDfO2vl28jQse6YU9PomJ8nx1Hc1Qmc9
YQt/2U3BG6wIOFf3TpXvHDRwtHzahwNy2G3qpd66O7sFjS1K4JuUePAH09GXeBGS
wHOPUc/TEXfyVBJEhpeFdxD4MOentl+c92L6zdfGMKaDujUuyH6zub5p7SrOEPtu
WSOCdGRp
=iPHs
-----END PGP MESSAGE-----

Wie sie unschwer am Ausschnitt des Quelltextes der Originalmail erkennen können, ist die Mail nur für den Empfänger, nicht aber für Dritte im Klartext lesbar. Voila.

Risiken aus Empfängersicht:
Sollten Sie die Passphrase oder den privaten Schlüssel verlieren, sind Mails, die mit dem öffentlichen Schlüssel verschlüsselt wurden, nicht mehr lesbar. Sorgfalt im Umgang mit beidem ist angesagt. Der Gewinn an Sicherheit und Vertrauen wiegt aus meiner Sicht diese Risiken auf, gerade sensible Informationen sollten immer verschlüsselt werden.

Zum Schluss

Sollte das vorliegende kleine Buch Ihnen beim Einstieg in geschützte Kommunikation geholfen haben, würde ich mich freuen. Es ist eine Umstellung, für Sie, aber auch für Ihre Kontakte. Zugegeben. Aber gerade die jüngsten Auseinandersetzung um die wichtige, nicht einfach zu beantwortende Frage, wieviel Sicherheit und wieviel Freiheit und Privatheit eine moderne, demokratische Gesellschaft benötigt, wird letztlich auch vom mündigen Bürger entschieden. Sie können und dürfen der Überwachung Grenzen setzen, auch und gerade im Interesse des demokratischen Rechtsstaats. Dass die Open Source Bewegung Ihnen diese Möglichkeit zur Verfügung stellt, ist ein großer Gewinn für alle.

Ein noch größerer Gewinn wäre aber, wenn die Regierungen der demokratisch regierten Staaten, sich auf gemeinsame Regelungen zum Datenschutz und zur Abgrenzung von Freiheits- und Sicherheitsaspekten einigen könnten. Erst dann wäre im Rahmen eines transparenten Gesetzgebungsverfahrens, das international anerkannt wäre, ein sicherer rechtlicher Rahmen für den Bürger gegeben. Bis zur Realisierung dieser schönen Vision müssen wir uns halt selbst helfen.

Bis dahin
Ihr Peter Dippold