Mails verschlüsseln mit Thunderbird

1. Voraussetzungen & Installation

Zum Verschlüsseln Ihrer E-Mails mit Thunderbird benötigen Sie zwei zusätzliche Programme: Das Verschlüsselungsprogramm „GPG“ (**Gnu Privacy Guard**) und das Thunderbird-Add-On „Enigmail“.

Enigmail lässt sich auf jedem System genau gleich installieren: Gehen Sie in das Anwendungsmenü, klicken Sie dort auf Add-Ons und suchen Sie nach **„Enigmail“**. Klicken Sie dann auf „Hinzufügen“ und bestätigen Sie. Für GPG müssen Sie je nach Betriebssystem eine andere Quelle nutzen: Unter Linux finden Sie GPG in Ihrem Paketmanager, meist unter dem Namen „**gpgv2“** oder **„gnupg“**. Für Windows können Sie **GPG4win** nutzen (https://www.gpg4win.org/download.html). Installieren Sie am besten die „Vanilla“-Version, mehr benötigen Sie nicht. Für Mac OS X gibt es die **GPGTools** (https://gpgtools.org/).

2. Einrichtung

Wenn Sie nun Thunderbird neu starten und auf den Menüpunkt **Enigmail** klicken, sollte sich automatisch der Assistent starten. Falls die Menüleiste am oberen Fensterrand nicht sichtbar ist, rechtsklicken Sie auf die Symbolleiste und aktivieren Sie den Punkt **„Menüleiste“**. Falls der Assistent nicht automatisch startet, klicken Sie auf **Enigmail** > **Einrichtungs-Assistent**. Wählen Sie die **Standard-Konfiguration** und danach „**Ich möchte ein neues Schlüsselpaar erzeugen“**. Wählen Sie nun die Mailadresse, mit der Sie verschlüsselte Mails versenden und empfangen wollen. Sie können später weitere Mailadressen hinzufügen. Wählen Sie ein starkes Passwort, das Sie nicht verlieren sollten. Ohne das Passwort haben Sie später keinen Zugriff mehr auf Ihre verschlüsselten Nachrichten. Wenn Sie auf **weiter** klicken, braucht Enigmail einige Minuten, um Ihre Schlüssel zu erstellen.

Ein **Widerrufszertifikat** können Sie erzeugen, wenn Sie sicher gehen wollen, dass niemand in Ihrem Namen E-Mails schreiben kann, falls Ihr privater Schlüssel einmal in fremde Hände fällt. Speichern Sie dieses Zertifikat an einem separaten Ort z.B. auf einem USB-Stick, den Sie getrennt von Ihrem Rechner aufbewahren. Das spätere In-Umlauf-Bringen des Widerrufszertifikats führt dazu, dass die E-Mail-Programme Ihrer Kontakte Ihrem Schlüssel nicht mehr vertrauen. Sie können dieses Zertifikat allerdings auch noch später erzeugen.

Enigmail ist nun fertig eingerichtet.

3. Schlüssel veröffentlichen

Bevor Ihnen jemand eine verschlüsselte Mail senden kann, benötigt er Ihren sogenannten **„öffentlichen Schlüssel“**. Diesen können Sie direkt beim Versenden an Ihre Mails anhängen, indem Sie beim Verfassen in der neu hinzugekommenen Enigmail-Leiste, über dem Adressfeld, auf **Meinen öffentlichen Schlüssel anhängen** drücken. Damit auch Personen, zu denen Sie bisher keinen Kontakt hatten, Ihnen verschlüsselte E-Mails schicken können, sollten Sie zusätzlich den öffentlichen Schlüssel auf einen Schlüsselserver hochladen. Dazu klicken Sie auf **Enigmail** > **Schlüssel verwalten...** und klicken Sie mit der rechten Maustaste auf Ihre Mailadresse und im erscheinenden Menü auf den Punkt **Auf Schlüsselserver hochladen...** .

4. Schlüssel importieren

Wie schon beim Veröffentlichen Ihrer eigenen öffentlichen Schlüssel gibt es zwei Möglichkeiten, die öffentlichen Schlüssel Anderer zu importieren, um diesen verschlüsselte Mails zu senden. Beachten Sie bitte, dass Sie dem Schlüssel einer Person erst vertrauen können, wenn Sie ihn über einen sicheren Kommunikationskanal, wie zum Beispiel ein persönliches Treffen mit Vergleich der Schlüssel, selbst verifiziert haben. Die im Schlüssel genannte E-Mail-Adresse ist **KEIN** Garant für die Echtheit des Schlüssels. Senden Sie also keine hochsensiblen Informationen an eine Person, solange Sie deren Identität nicht durch einen sicheren Kanal sichergestellt haben.

Hat Ihnen jemand seinen Schlüssel per Mail gesendet, klicken Sie darauf mit der rechten Maustaste (die Datei im Anhang hat meist einen kryptischen Namen wie beispielsweise „0xAB34C98.asc“) und wählen Sie **OpenPGP-Schlüssel importieren**.

Wenn Sie nur die Mailadresse einer Person kennen, jedoch wissen, dass Sie Ihren öffentlichen Schlüssel auf einem Schlüsselserver veröffentlicht hat, können Sie auch auf dem Server nach dem Schlüssel suchen und ihn von dort importieren. Dazu klicken Sie auf **Enigmail** > **Schlüssel verwalten...** und klicken im erscheinenden Fenster auf **Schlüsselserver** > **Schlüssel suchen...** . Wenn der Schlüssel schon länger existiert können Sie einen beliebigen Server nehmen, wurde der Schlüssel gerade erst erstellt, sollten Sie ihn von dem Server importieren, auf den er als erstes hochgeladen wurde. Mit der Zeit bringen sich alle Schlüsselserver gegenseitig auf den aktuellsten Stand. Geben Sie nun in das Suchfeld die E-Mail-Adresse ein, zu der Sie einen Schlüssel suchen. Nach wenigen Minuten sollte der Schlüssel gefunden sein und Sie können ihn importieren, indem Sie in der Zeile mit der Mailadresse vorne ein Häkchen setzen und dann auf **OK** klicken.

5. Senden und Empfangen

Möchten Sie eine verschlüsselte Nachricht schicken, schreiben Sie wie gewöhnlich eine E-Mail, klicken Sie jedoch vor dem Versenden auf das **Schlosssymbol** oben in der Leiste. Wenn Sie gegenüber Anderen zudem verifizieren möchten, dass Sie der Absender der Nachricht waren, klicken sie auf das **Stiftsymbol** daneben. Dies erzeugt eine digitale Unterschrift Ihrer Nachricht. Jetzt können Sie Ihre Nachricht verschicken, Sie werden lediglich noch einmal nach der Passphrase gefragt, mit der Sie Ihr Schlüsselpaar gesichert haben.

Das Empfangen einer verschlüsselten Nachricht ist sogar noch leichter. Wenn Sie die Nachricht aufrufen, werden Sie von Enigmail automatisch nach der Passphrase gefragt. Geben Sie diese ein, wird Ihnen die entschlüsselte Nachricht angezeigt. Ein Hinweis: das Ver- und Entschlüsseln großer Anhänge kann sehr lange dauern, daher fragt Sie Enigmail beim Versenden von Anhängen, ob Sie diese auch verschlüsseln bzw. unterschreiben wollen. Bei großen Dateien, die nicht sensibel sind, können Sie diese unverschlüsselt, jedoch signiert, versenden, sodass zumindest sichergestellt werden kann, dass die Dateien unterwegs nicht manipuliert wurden. Den Text sollten Sie in jedem Fall verschlüsseln.

Eine **Videoserie** zu Enigmail finden Sie auch unter folgendem Link:
https://www.youtube.com/playlist?list=PL3-bM7Aq1pUr8wiX4XFW1hxvH1SlfBtsT