

INSTALLATION ENIGMAIL

1. Thunderbird mit Internetverbindung starten
2. Extras - Addons - Erweiterungen
3. alle Addons durchsuchen nach „Enigmail“ - aus Liste auswählen
4. Enigmail installieren
5. Thunderbird neustarten
6. Enigmail ist nun in Menüleiste eingetragen

AB HIER STARTET DIE KONFIGURATION

7. Enigmail anklicken, Einrichtungsassistent anklicken
8. zur Auswahl stehen :
 - Standard-Konfiguration für Anfänger
 - ausführliche Konfiguration für Fortgeschrittene
 - manuelle Konfiguration für Experten-Einstellungen
 - aus vorheriger Installation importieren

ICH GEHE ZUNÄCHST DIE MANUELLE KONFIGURATION DURCH :

1. zur Auswahl stehen
 - Schlüssel-Manager und
 - Experten-Einstellungen - und das wird ausgewählt
2. Allgemein
 - Dateien und Verzeichnisse gefunden → GnuPG in /usr/bin/gpg2
 - nicht überschreiben
 - Passphrase 5min merken
 - nie nach einer Passphrase fragen - nein
3. Senden
 - für Verschlüsselung → Standardeinstellung - ja
 - manuell einrichten - nein
 - automatisch verschlüsselt senden → wenn möglich ja
 - um verschlüsselt zu senden, akzeptiere → alle verwendbare Schlüssel
 - Senden bestätigen → nie
4. Schlüsselauswahl
 - durch Mailadresse gemäss Schlüsselverwaltung → ja
 - durch Empfängerregeln
 - manuell, falls Schlüssel fehlen
 - immer manuell
5. Weitere Einstellungen
 - Betreff verschlüsseln - nein
 - Betrefftext zum Schutz verschlüsselter Nachrichten wählen - wenn gewünscht
 - signierten HTML-Text vor Senden umbrechen - ja
 - Enigmail-Kommentar zur OpenPGP-Signatur hinzufügen - wenn gewünscht
 - „ - “ Signatur-Trenner
 - „< >“ kennzeichnet MailAdresse
 - Anhänge herunterladen, wenn diese geöffnet werden sollen (nur bei IMAP)
 - Warnungen zurücksetzen
6. Schlüsselservers
 - angeben falls gewünscht, aber
 - man bedenke: Schlüssel können aus dem Server nicht mehr gelöscht werden
7. Einstellungen übertragen
 - entweder Autocrypt-Schlüsselübertragung oder
 - Übertragung in einer ZIP-Datei, dazu auswählen
 - Einstellungen und Schlüssel exportieren oder
 - Einstellungen und Schlüssel wiederherstellen
8. damit ist die manuelle Konfiguration beendet, der Punkt 9 bezieht sich auf Konfiguration der Thunderbird-Konteneinstellungen

9. an dieser Stelle erfolgt ein Ausflug in die Thunderbird-Konteneinstellungen
 dieser Aufruf muss für jedes Mailkonto einzeln gemacht werden
 Konteneinstellungen anklicken → OpenPGP-Sicherheit anklicken
 GnuPG muss installiert sein
 aktiviere OpenPGP-Unterstützung
 Mailadresse zur Identifizierung von OpenPGP-Schlüssel verwenden
 Standard-Einstellungen für Verfassen → PGP/MIME verwenden
 Entwürfe verschlüsselt speichern
 wenn Enigmail- oder S/MIME-Verschlüsselung möglich ? → Enigmail-Verschlüsselung wählen

NUN FOLGT DIE AUSFÜHRLICHE KONFIGURATION MIT SCHLÜSSELERSTELLUNG :

1. welche Konten sind betroffen ?
 vorhandene Konten sind aufgelistet → die betroffenen ankreuzen
 Hinweis: egal was man ankreuzt, es werden alle Konten verwendet ! hi-hi
2. neues Schlüsselpaar
 aus Datei importieren - falls vorhanden, sonst nein
 erzeugen → ja
3. Information über die zu erzeugenden Schlüssel
 öffentlicher Schlüssel → Sender und Empfänger tauschen ihren „Öffentlichen“ aus und verschlüsseln damit ihre Mails untereinander, die „Öffentlichen“ werden in der Schlüsselverwaltung eingetragen
 privater Schlüssel → damit lese ich verschlüsselte Mails von Anderen an mich, oder ich signiere Mails, die ich verschicke
4. Passphrase erstellen (min 8 Zeichen, Ziffern, Satzzeichen, keine Umlaute ö-ä-ü)
 diese Passphrase schützt meinen privaten Schlüssel und wird zum Entschlüsseln verwendet, d.h. es wird nicht wirklich der private Schlüssel verwendet sondern genau genommen die Passphrase !
5. im Folgenden wird das Schlüsselpaar (öffentlich, privat) erzeugt.
 dazu sind Aktivitäten im Internet oder an Dateien solange nötig, bis die Meldung „Schlüssel erzeugt“ ausgegeben wird.
6. zur Sicherung des privaten Schlüssels (Verlust, Diebstahl), Widerrufs-zertifikat erstellen (empfohlen)
 es erklärt den öffentlichen Schlüssel für ungültig
 dazu muss die Passphrase eingegeben werden
 erstellt wird eine Datei „name-rev.asc → Datei sicher speichern (rev=revoke=Widerruf)
7. wie gebe ich meinen öffentlichen Schlüssel weiter ?
 angeboten wird, ihn auf einen Schlüssel-Server hochzuladen
 (ein hochgeladener Schlüssel kann nicht mehr vom Server gelöscht werden !) oder den Schlüssel an meine Mail anhängen → gewählt
8. Enigmail ist nun fertig eingerichtet

TEST EINER MAILVERSCHLÜSSELUNG :

1. Enigmail - Schlüssel verwalten.... erstmal reinschauen ob der „Öffentliche“ des Mailempfängers vorhanden ist.
2. wenn nicht - Schlüssels-server - Schlüssel suchen....
3. Vorname Name - Rufzeichen - Mailadresse , irgendsowas oder als ZIP-Datei anfordern
4. wenn der „Öffentliche“ dann endlich vorliegt → neue Nachricht verfassen
5. Schloss-Symbol anklicken, Verschlüsselung EIN
6. Enigmail - den Schlüssel aller Empfänger vertrauen, aktivieren und
7. meinen öffentlichen Schlüssel anhängen, aktivieren
8. Senden anklicken
9. der Empfänger sieht den Posteingang und öffnet die Mail
10. nun aber wird die Passphrase des Mail-Empfängers abgefragt - einfach eingeben
11. und schon erscheint die Nachricht im Klartext