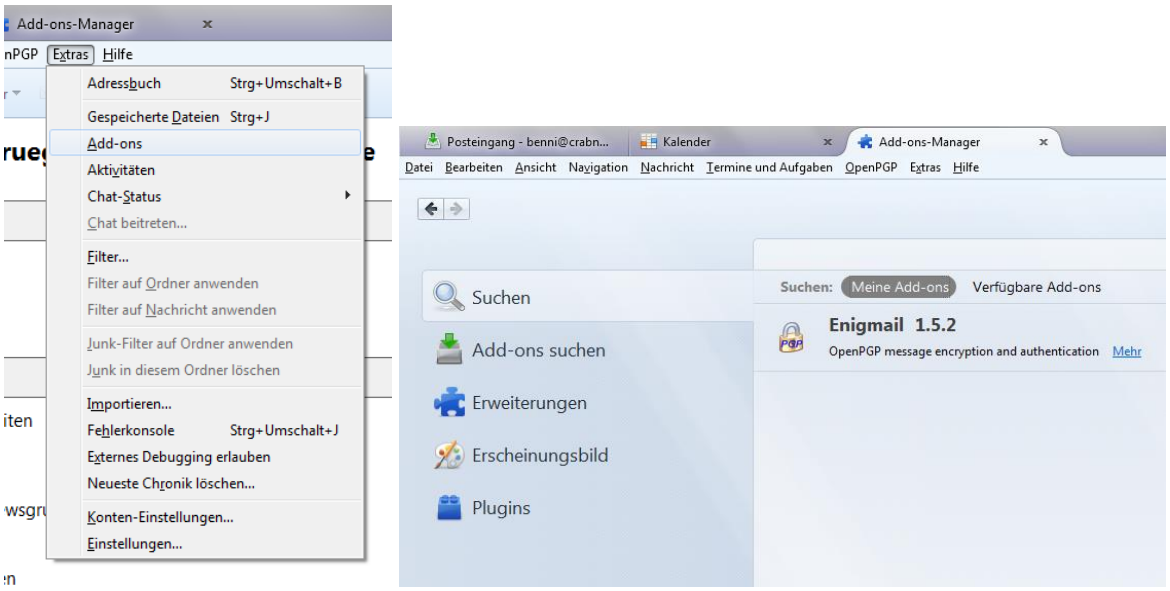
Wie richte ich eine PGP-Verschlüsselung mit Mozilla Thunderbird ein?

Folgende Anleitung wurde unter Windows 7 mit der Thunderbird Version 24.0.1, gpg4win 2.2.1 und Enigmail 1.5.2 erstellt. Bei anderen Programmversionen sind Abweichungen möglich.

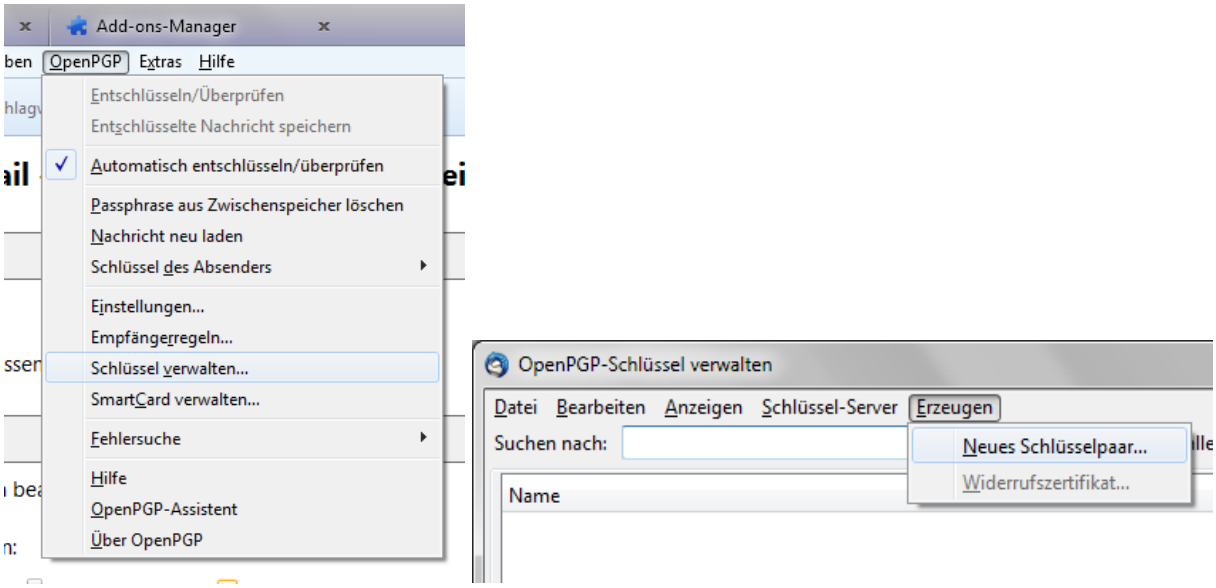
1. Sofern nicht schon geschehen, das Paket „gpg4win“ installieren. (http://www.gpg4win.de). Eine detaillierte Anleitung dafür finden Sie auf unseren Seiten. (https://www.internet-sicherheit.de/pgpzi/)

2. Thunderbird installieren und die E-Mail Konten konfigurieren. (sofern nicht schon geschehen)

3. In Thunderbird im Menü „Extras“ den Add-ons-Manager öffnen. Dort nach dem Add-on „Enigmail“ suchen und hinzufügen. Wenn Enigmail während der Installation nach einer Version von GnuPG fragen sollte, suchen sie auf ihrem Computer nach der Datei „gpg.exe“ oder „gpg2.exe“ und geben sie diesen Pfad an.



4. Falls Sie noch keinen Schlüssel haben, müssen Sie nach dem benötigten Neustart von Thunderbird über das Menü „OpenPGP“->„Schlüssel verwalten“ via „Erzeugen“->„Neues Schlüsselpaar“ ein neues Schlüsselpaar erzeugen. Befolgen Sie dazu folgende Schritte:



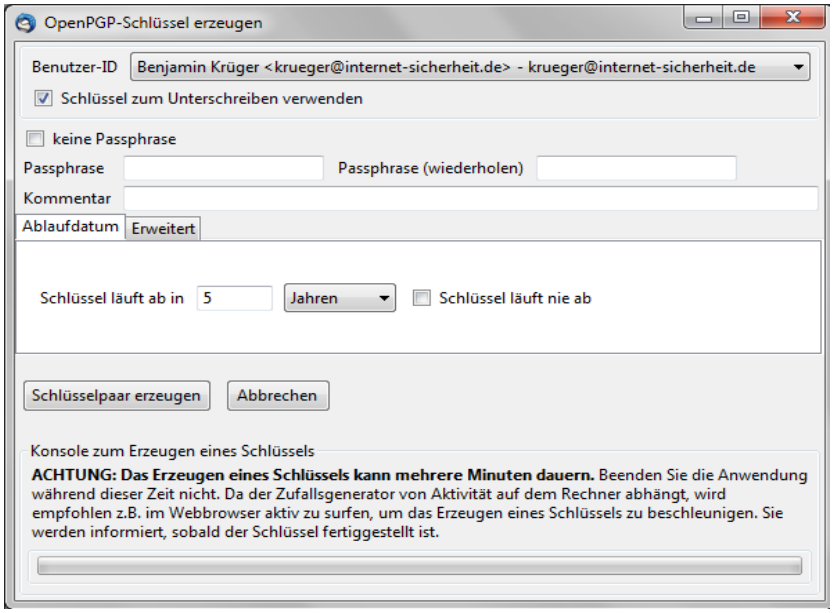
a) Die Benutzer-ID für den GPG Schlüssel auswählen (Ihre E-Mail-Adresse).

b) Häkchen setzen bei „Schlüssel zum Unterschreiben verwenden“.

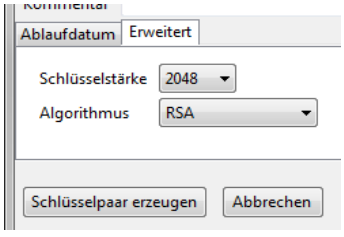
c) Passphrase für den Schutz des privaten Schlüssels zweimal eingeben.
Beachten Sie bei der Erstellung der Passphrase die if(is)-Checkliste zur Erstellung sicherer Passwörter!
http://www.it-sicherheit.de/ratgeber/checklisten_it_sicherheit/checkliste/checkliste-verwende-ich-sichere-passwoerter/

d) (Optional) Kommentar zum Schlüssel eingeben.

e) Es wird empfohlen, Den Schlüssel nach ein paar Jahren ablaufen zu lassen. Wenn der Schlüssel verloren geht, läuft er so automatisch aus. Zudem kann man einen abgelaufenen Schlüssel ohne weiteres verlängern.



f) Im „Erweitert“-Tab ist standardmäßig eine Schlüsselstärke von 2048 Bit eingestellt. Dies ist zwar derzeit noch ausreichend, aufgrund der stetig wachsenden Rechenleistung von PCs ist es ratsam, schon eine Schlüssellänge von 4096 Bit zu benutzen. Ein nachträgliches Ändern der Schlüsselstärke ist nicht möglich.



g) Mit einem Klick auf „Schlüsselpaar erzeugen“ wird das Schlüsselpaar erzeugt.

5. Im Anschluss daran sollte der Schlüssel auf einen Keyserver hochgeladen werden, damit andere Personen den öffentlichen Schlüssel zum Verschlüsseln nutzen können. Sie können dazu selbstverständlich die PGP-Zertifizierungsinstanz des if(is) nutzen. https://www.internet-sicherheit.de/pgpzi/

6. Um die Nachricht nun zu verschlüsseln, erstellt man einfach eine neue E-Mail.

7. Der Shortcut zum Verschlüsseln ist <STRG> + <SHIFT> + E

Der Shortcut zum Signieren ist <STRG> + <SHIFT> + S

Alternativ kann man im Menü auch auswählen ob eine Nachricht verschlüsselt und/oder signiert werden soll. Ebenso ist auch ein Click auf die beiden Icons in der unteren rechten Ecke des E-Mail-Fensters möglich. In den Kontoeinstellungen können Sie auch standardmäßig einstellen, ob eine E-Mail immer unterschrieben oder verschlüsselt werden soll.