## 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. (<u>http://www.gpg4win.de</u>). Eine detaillierte Anleitung dafür finden Sie auf unseren Seiten. (<u>https://www.internet-sicherheit.de/pgpzi/</u>)

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:

ben OpenPGP Extras Hilfe hlagv Entschlüsseln/Überprüfen Entschlüsselte Nachricht speichern Automatisch entschlüsseln/Überprüfen Passphrase aus Zwischenspeicher löschen	
hlagy     Entschlüsseln/Überprüfen       Entschlüsselte Nachricht speichern       Automatisch entschlüsseln/Überprüfen       Passphrase aus Zwischenspeicher löschen	
ail  Automatisch entschlüsseln/überprüfen ei Passphrase aus Zwischenspeicher löschen	
Passphrase aus Zwischenspeicher löschen	
Nachricht neu laden       Schlüssel des Absenders	
Einstellungen Empfängerregeln	
SSER Schlüssel verwalten	
Eehlersuche     Datei     Bearbeiten     Anzeigen     Schlüssel-Server     Erzeugen       Keules     Suchen nach:     Neues     Neues     Schlüssel-Server     Neues	selpaar ille
I bea Hilfe Name Widerrufszertif	fikat
n: Über OpenPGP	

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! <u>http://www.it-sicherheit.de/ratgeber/checklisten\_it\_sicherheit/checkliste/checkliste-verwende-ich-sichere-passwoerter/</u>

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.

(C) OpenPGP-	Schlüssel erzeugen							
Benutzer-ID	Benjamin Krüger <krueger@internet-sicherheit.de> - krueger@internet-sicherheit.de</krueger@internet-sicherheit.de>							
Schlüsse	Schlüssel zum Unterschreiben verwenden							
keine Pass	sphrase							
Passphrase	Passphrase (wiederholen)							
Kommentar								
Ablaufdatum	Erweitert							
Schlüssel läuft ab in 5 🛛 Jahren 👻 🔲 Schlüssel läuft nie ab								
Schlüsselpaar erzeugen Abbrechen								
Konsole zum Erzeugen eines Schlüssels ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.								

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.

Kunnentai	
Ablaufdatum	Erweitert
Schlüsselsta Algorithmu	irke 2048 🔻
Schlüsselpaa	r erzeugen Abbrechen

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. <u>https://www.internet-sicherheit.de/pgpzi/</u>

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.

				1011		
ť	🕝 Verfassen: (kein Betre	ff)				
v.	🎬 Senden 🛛 🖌 Rechtschr. 🔻 🛡 Anhang 🔻			🔒 OpenPGP 🔽 🔒 S/MIME 🔻 🔚 Speichern 🔻		
v	<u>V</u> on:	Benjamin Krüger < kruege		Nachricht unterschreiben Strg+Umschalt+S fe	-	
V	▼ An:	8		Nachricht verschlüsseln Strg+Umschalt+E		
L				PGP/MIME verwenden		
:				Empfängerregeln ignorieren		
	Bet <u>r</u> eff:		_			
22					^	
j					Ŧ	
l				I D	at	