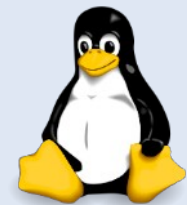


Workshop: Email-Verschlüsselung



Tagesordnungspunkte

- Begrüßung und Einführung
- Teilnehmer-Umfrage
- Thunderbird mit Enigmail / GPGP einrichten
- Schlüsselverwaltung
- Sicherung
- Mails schreiben, verschlüsseln und signieren, entschlüsseln und lesen
- Situationsabhängige Unterstützung individuell oder in kleinen Arbeitsgruppen, Demonstration



Workshop: Emailverschlüsselung



Grundlagen

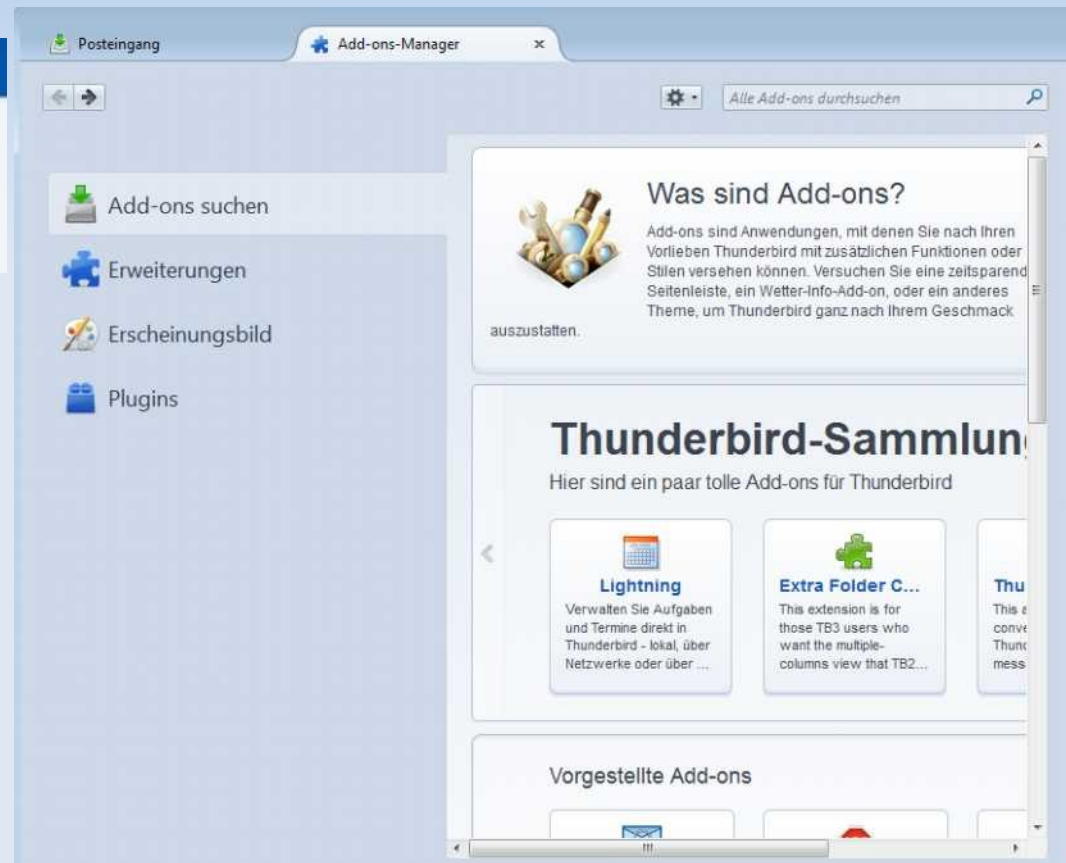
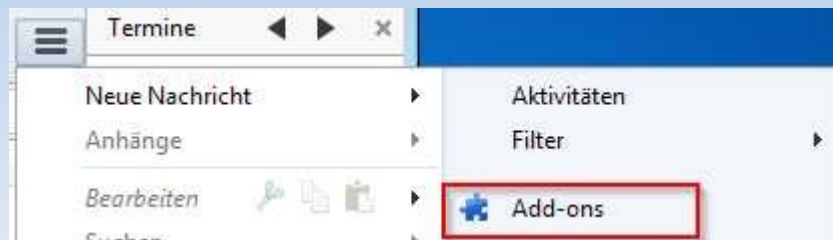
- Asymmetrische Verschlüsselung
- Public-Key-Verfahren
- Besteht aus einem privaten und einem öffentlichen Schlüssel
- Privater Schlüssel bleibt immer bei mir! (Sicherheit!)
- Öffentlicher Schlüssel als Datei, auf Schlüsselservers oder Text
- Verschlüsselung mit öffentlichem Schlüssel
- Entschlüsselung mit privatem Schlüssel

Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on)



Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on)

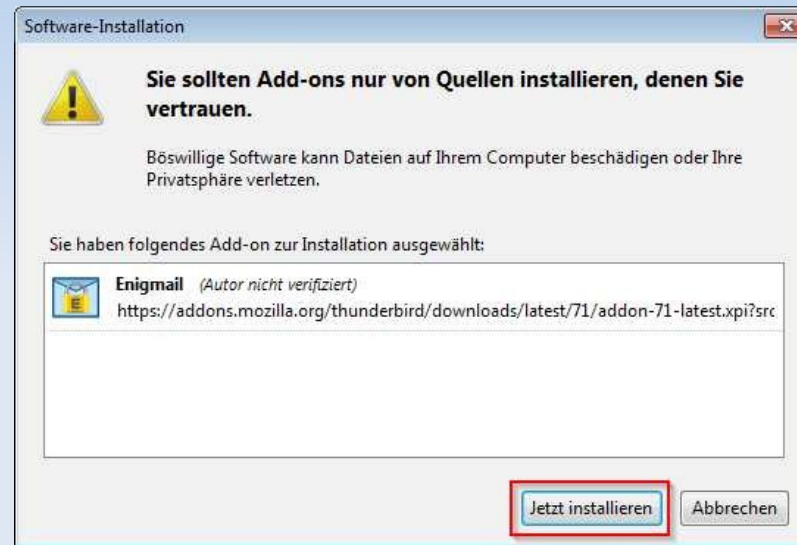
A screenshot of the Enigmail 1.8.2 add-on page for Thunderbird. The page features a blue header with the Enigmail logo and the text 'Enigmail 1.8.2 von Patrick Brunschwig'. Below this, a description reads 'Verschlüsseln und Authentifizieren von Nachrichten mit OpenPGP. Benötigt...' (partially visible). A prominent green button with a white plus sign and the text 'Zu Thunderbird hinzufügen' is highlighted with a red border. To its right is a grey button labeled 'mehr erfahren...'. Below the buttons is a screenshot of the Enigmail interface within the Thunderbird email client. At the bottom of the page, the rating is shown as 'Bewertung' with four yellow stars and the text '184 Bewertungen', and the number of active users is listed as 'Aktive Nutzer 140.744'.

Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on)

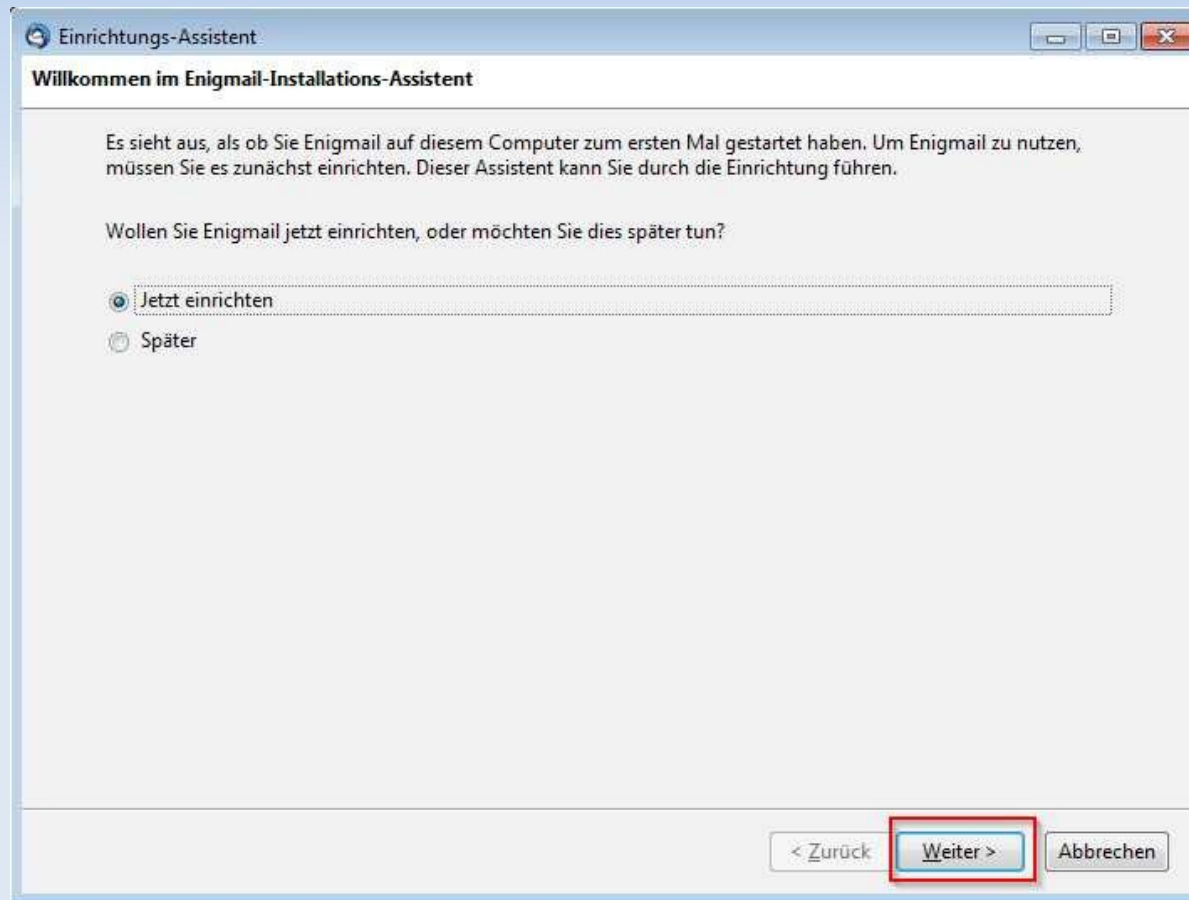


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail

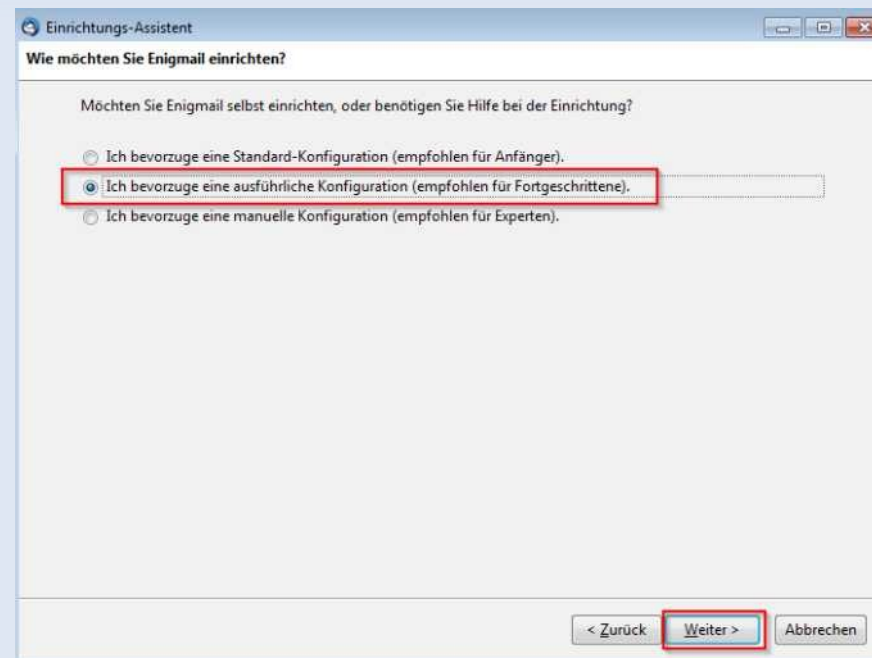


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail
- GnuPGP wird bei ausführen des Einrichtungs-Assistenten von Enigmail geprüft und selbständig heruntergeladen und installiert.

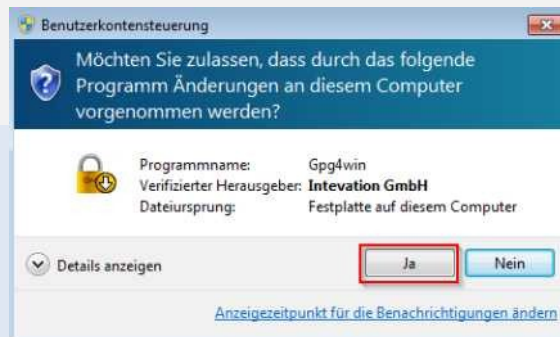
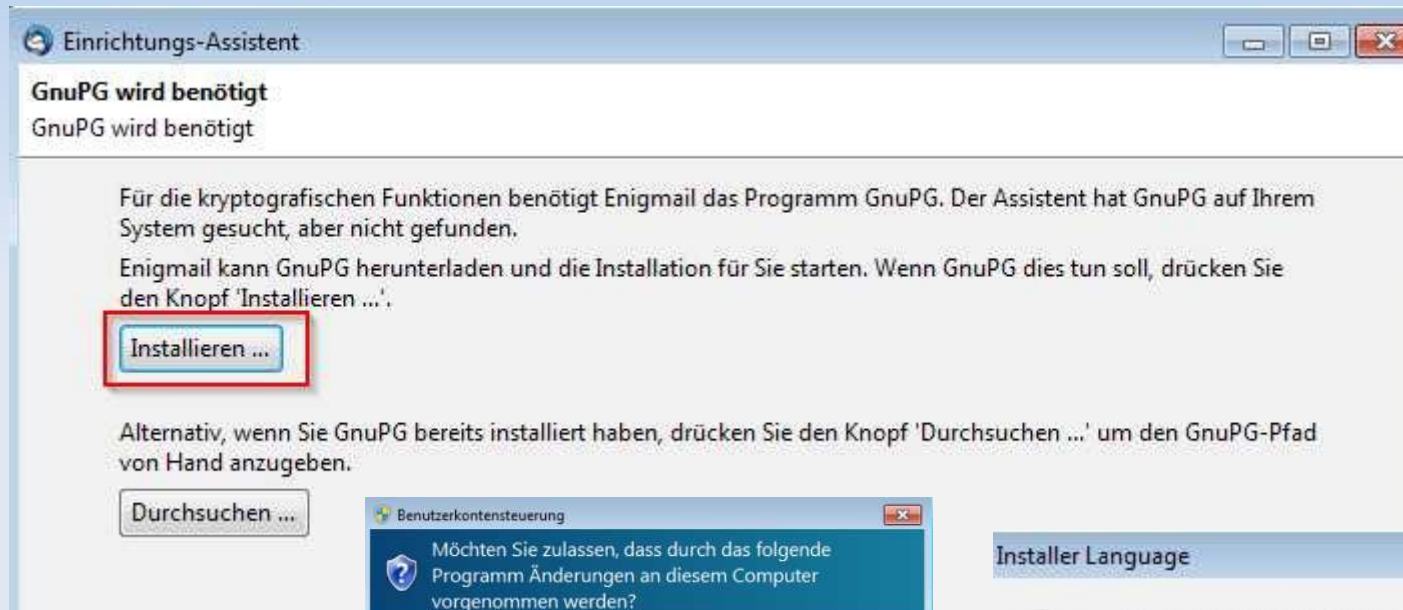


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG

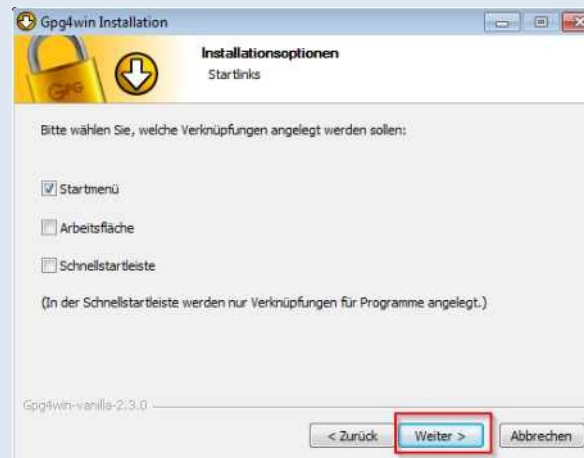


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG

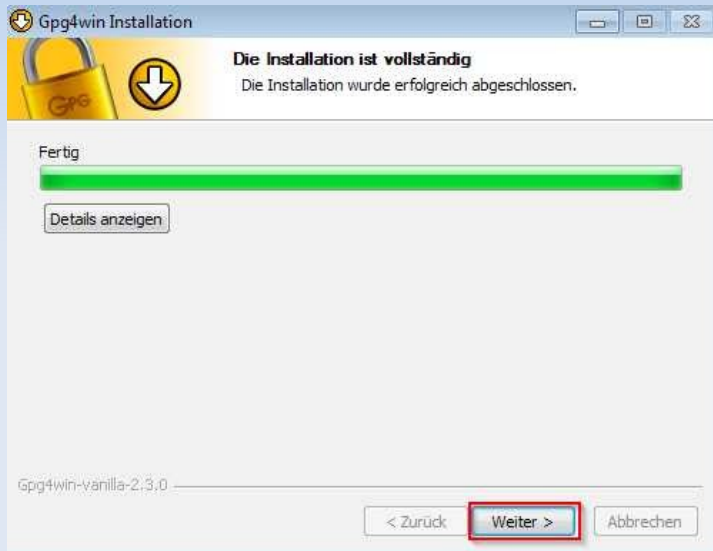


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG

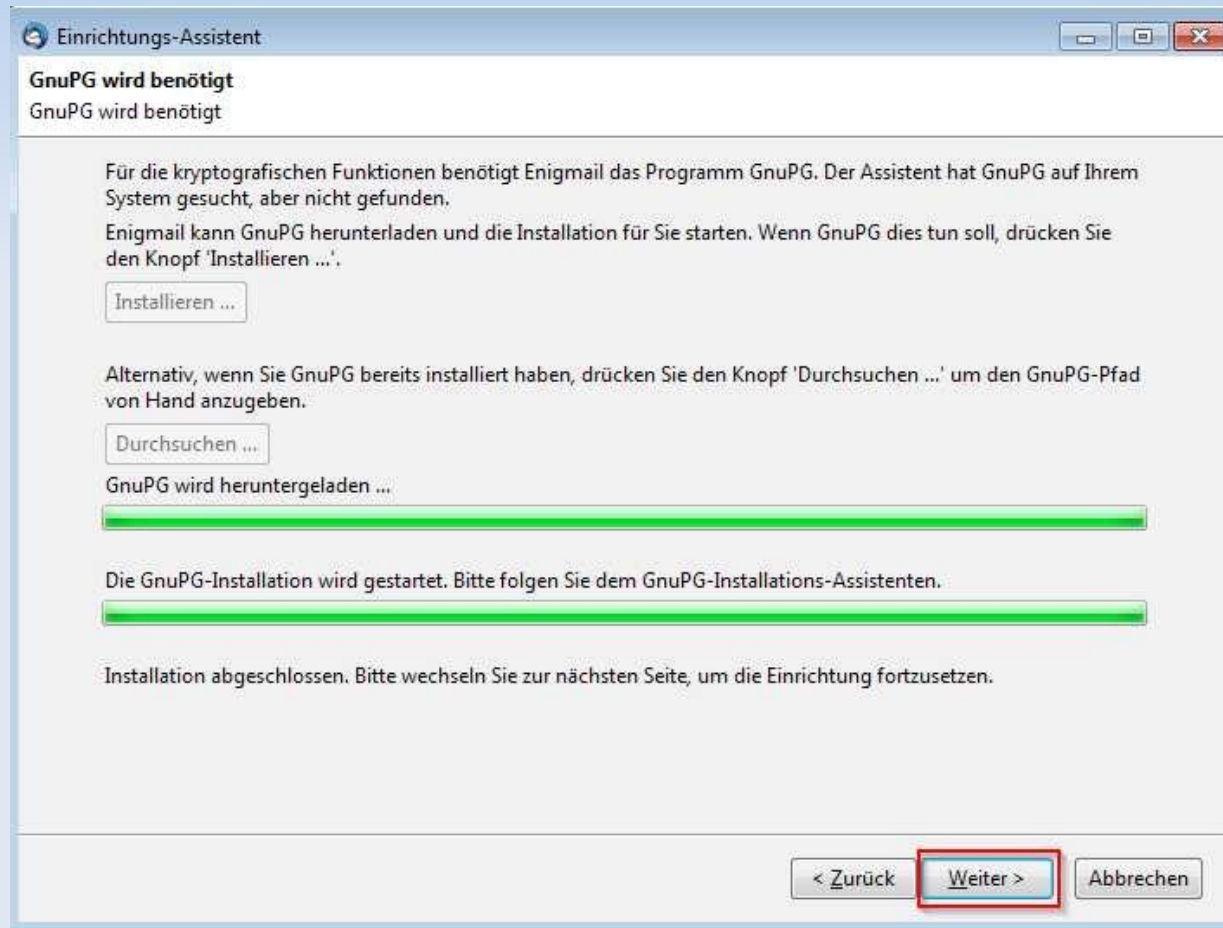


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)

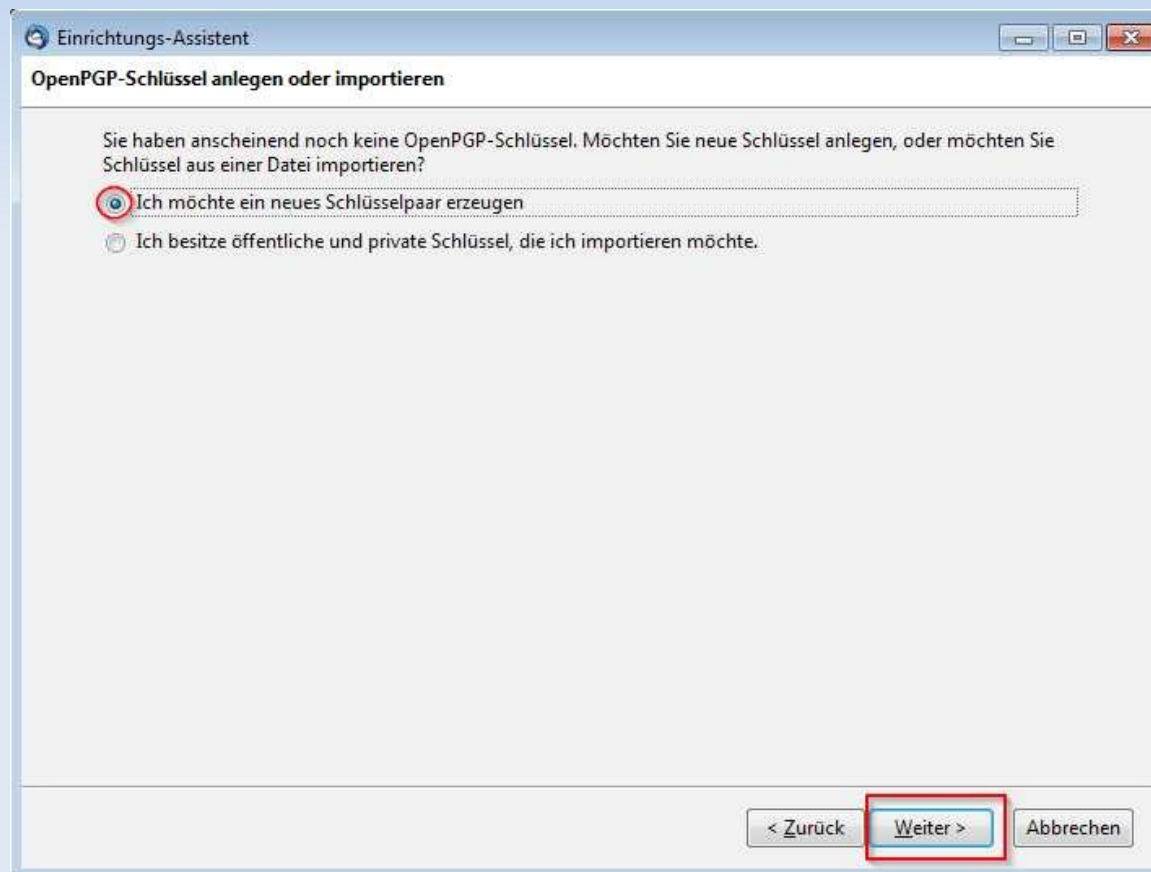


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)





Workshop: Emailverschlüsselung

Einrichtungs-Assistent

- Enigmail (Fortsetzung)

Einrichtungs-Assistent

OpenPGP-Schlüssel erzeugen
Erzeugen eines Schlüssels zum Unterschreiben und Verschlüsseln


Dieser Dialog wird ein Paar von zwei Schlüsseln anlegen:
Mit Ihrem **öffentlichen Schlüssel** können **Andere** Mails an Sie verschlüsseln (und von Ihnen unterschriebene Nachrichten prüfen). Sie dürfen ihn jedem geben.
Ihr **geheimer, privater Schlüssel** ist **nur für Sie**, um damit Mails an Sie zu entschlüsseln (und um Mails, die Sie schicken, zu unterschreiben). Diesen Schlüssel halten Sie geheim, Sie geben ihn niemandem.

Ihre **Passphrase** ist ein Passwort, mit dem GnuPG Ihren privaten Schlüssel schützt. Es soll Missbrauch Ihres privaten Schlüssels verhindern. Die Passphrase sollte ein Satz aus mindestens 8 Zeichen, Ziffern und Satzzeichen sein. Umlaute und andere sprachenspezifische Zeichen, zum Beispiel ä, é, ñ, sind **nicht** empfehlenswert (weil nicht jedes Programm damit richtig umgeht).

Konto / Benutzerkennung:
Beat U. <beat.uerlinger@zoho.com> - beat.uerlinger@zoho.com

Passphrase
●●●●●●●●

Bitte bestätigen Sie Ihre Passphrase durch erneutes Eingeben
●●●●●●●●

Qualität der Passphrase:


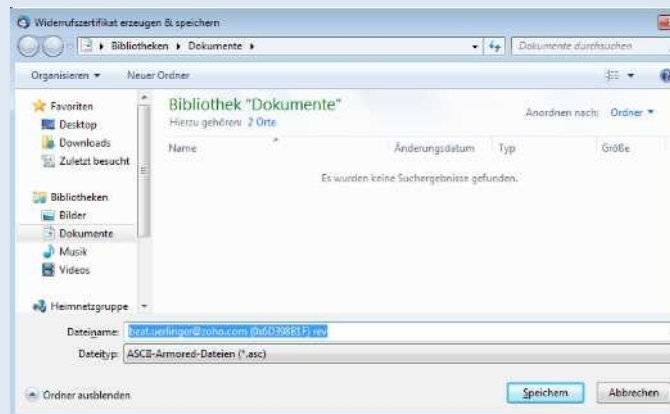
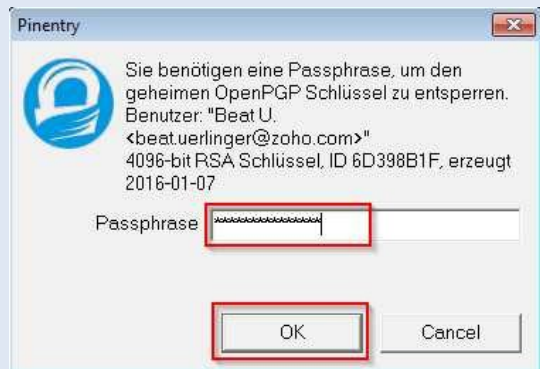
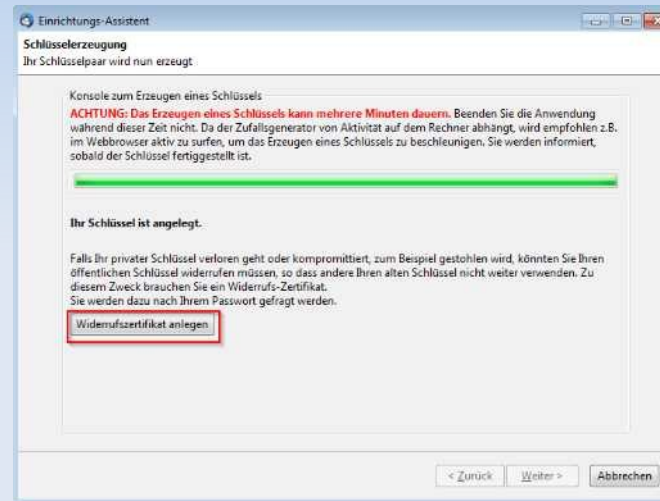
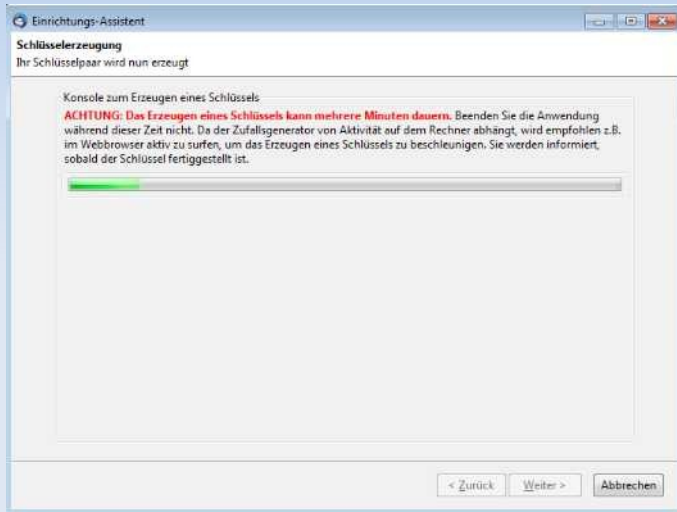
< Zurück Weiter > Abbrechen

Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)

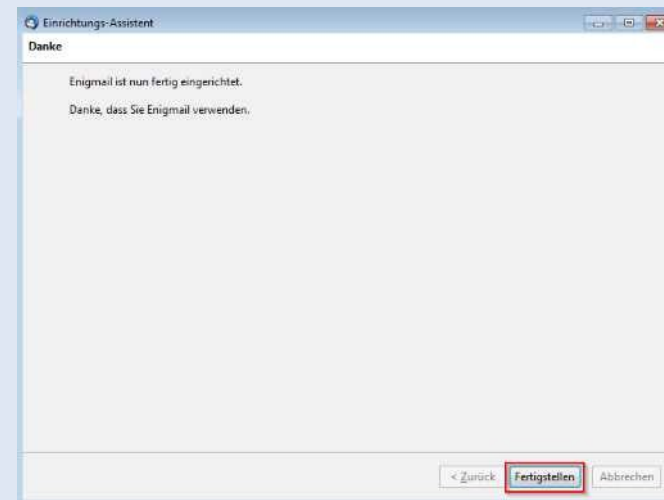
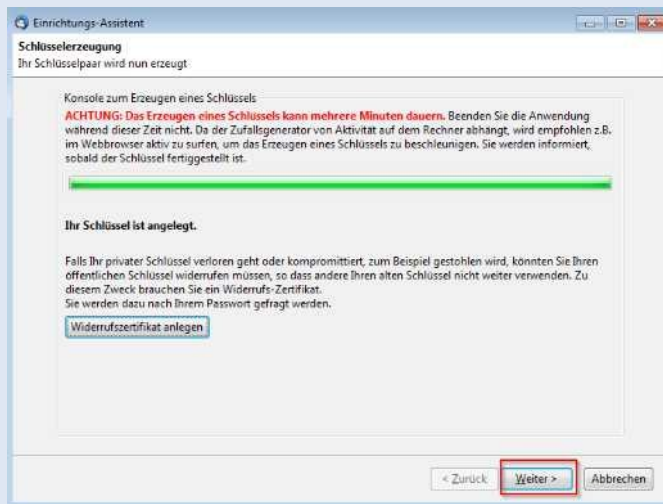
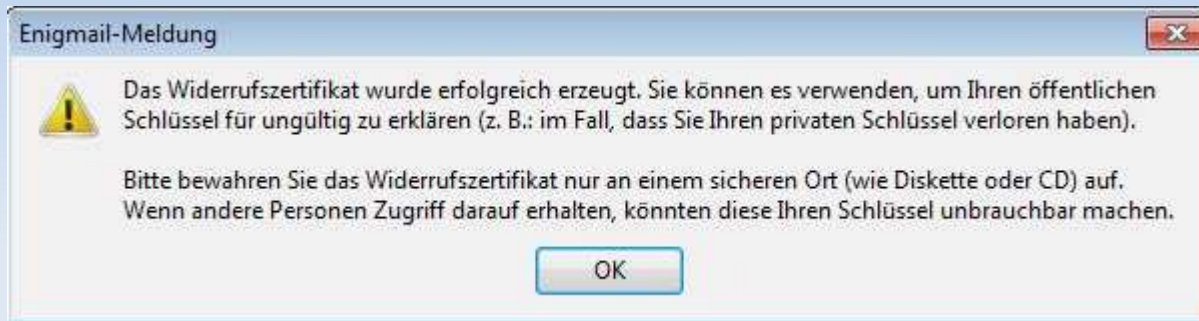


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)

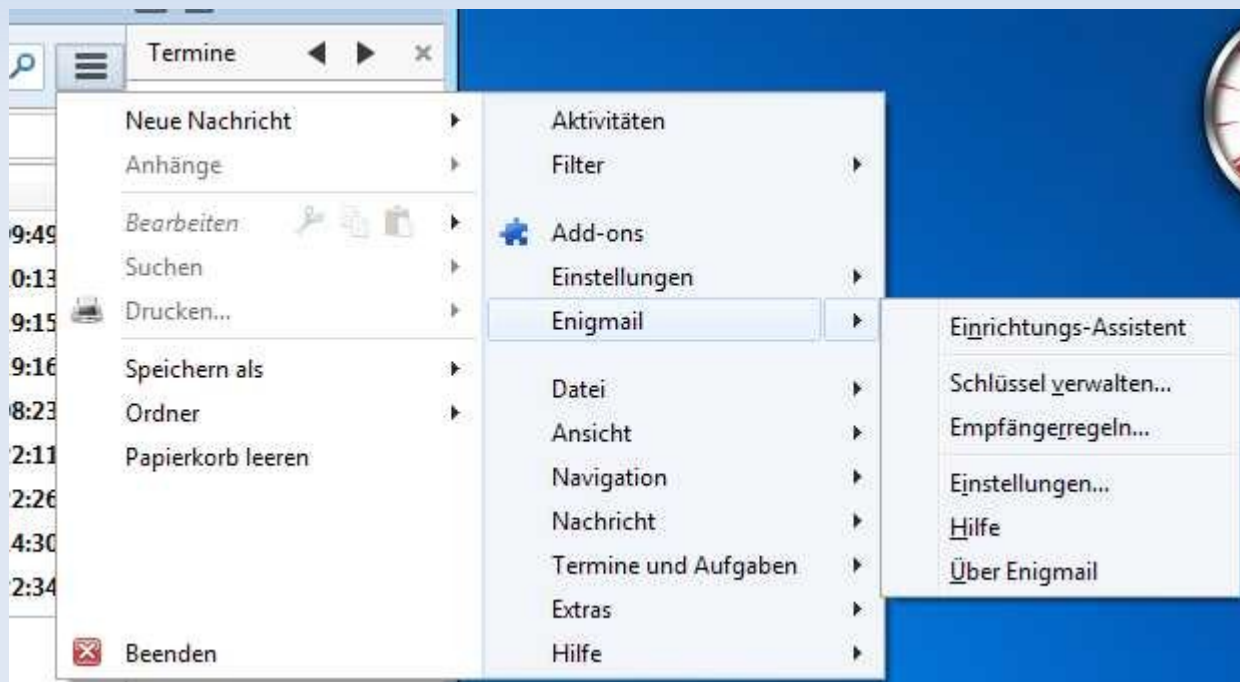


Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on) benutzen

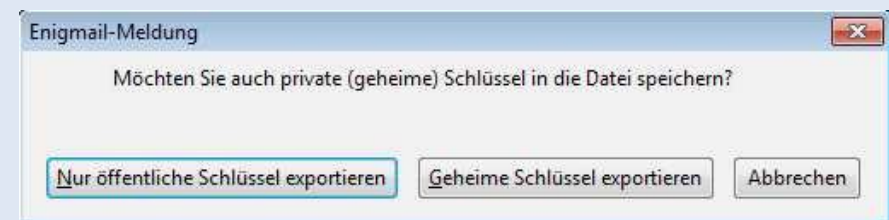
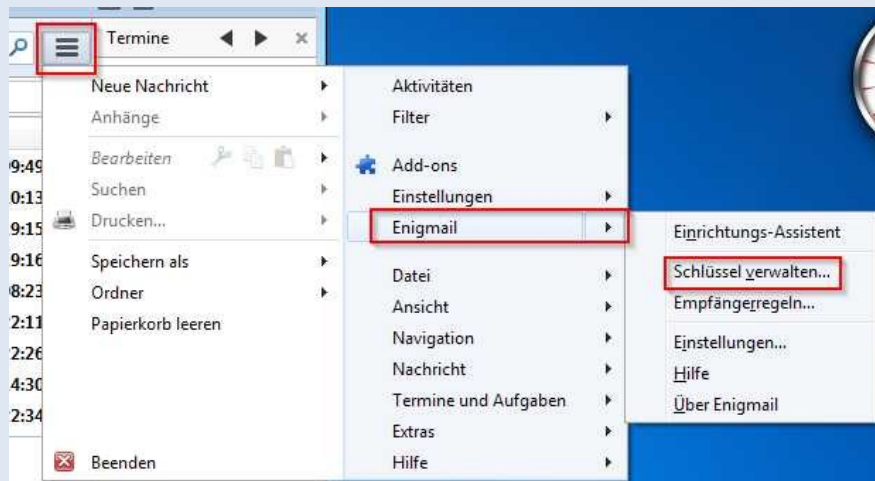


Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel importieren, exportieren, sichern
 - Fremde Schlüssel importieren
 - Eigenen Schlüssel exportieren oder sichern
 - Widerrufszertifikat erzeugen

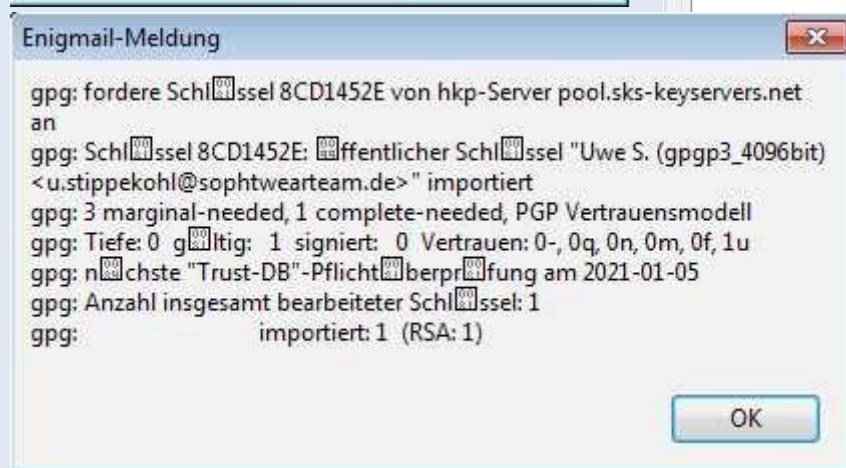
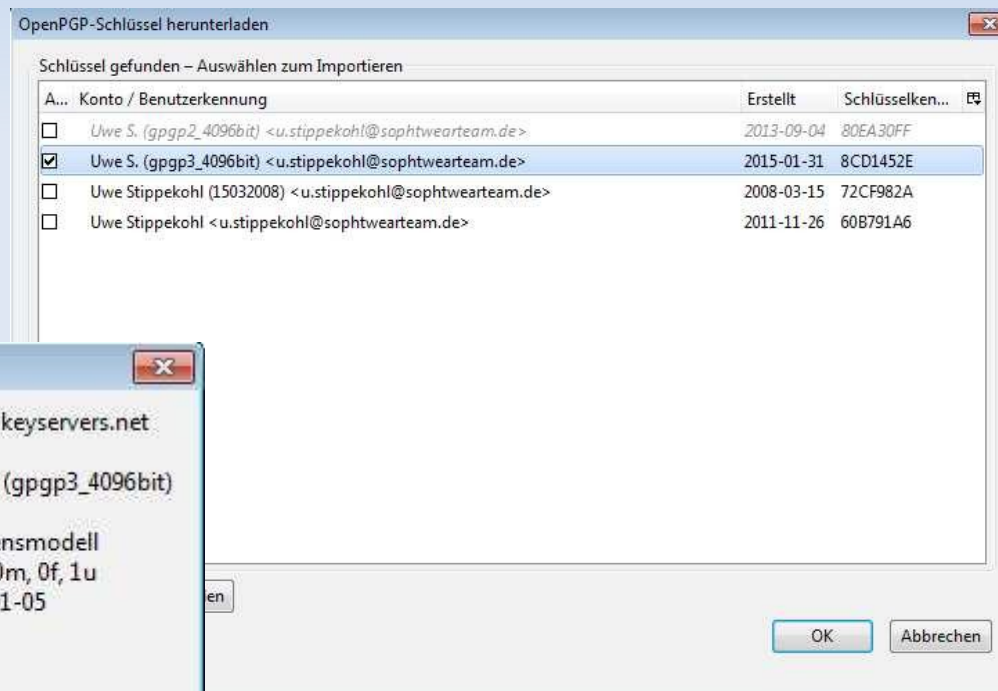


Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel importieren
 - Fremde Schlüssel importieren

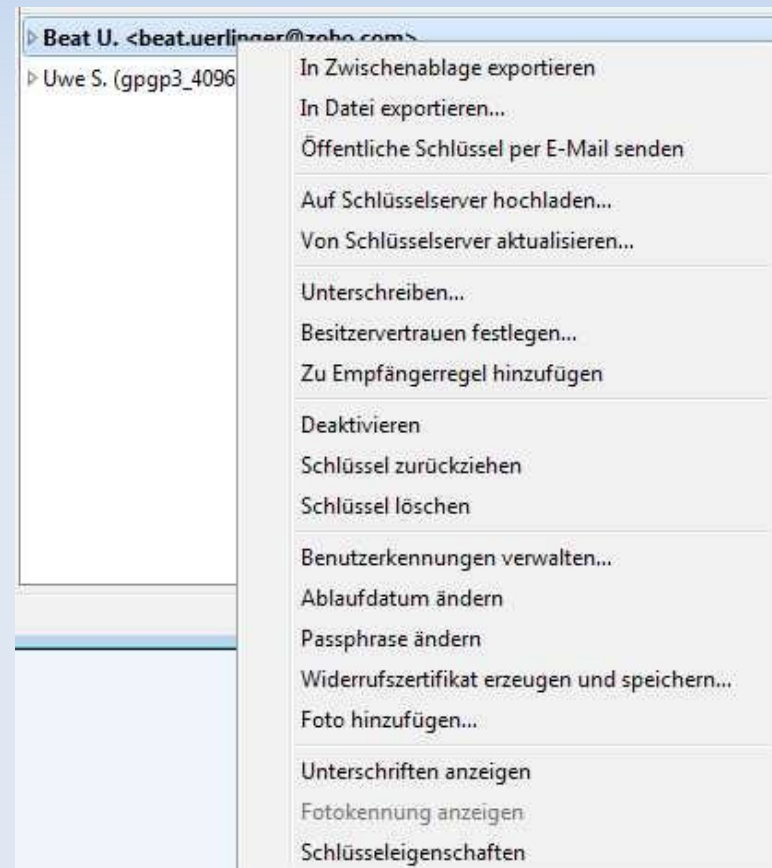


Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel exportieren
 - Eigenen Schlüssel exportieren oder sichern

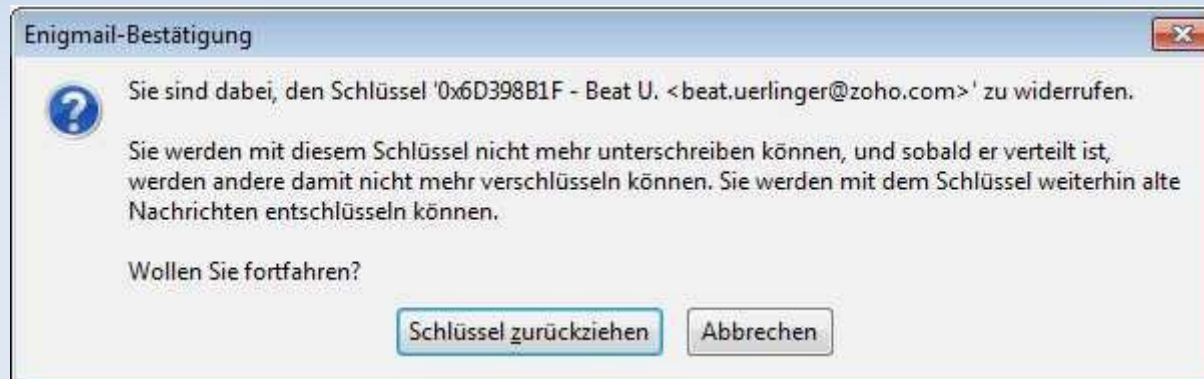


Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel importieren, exportieren, sichern
 - Widerrufs-zertifikat anwenden, Schlüssel zurückziehen

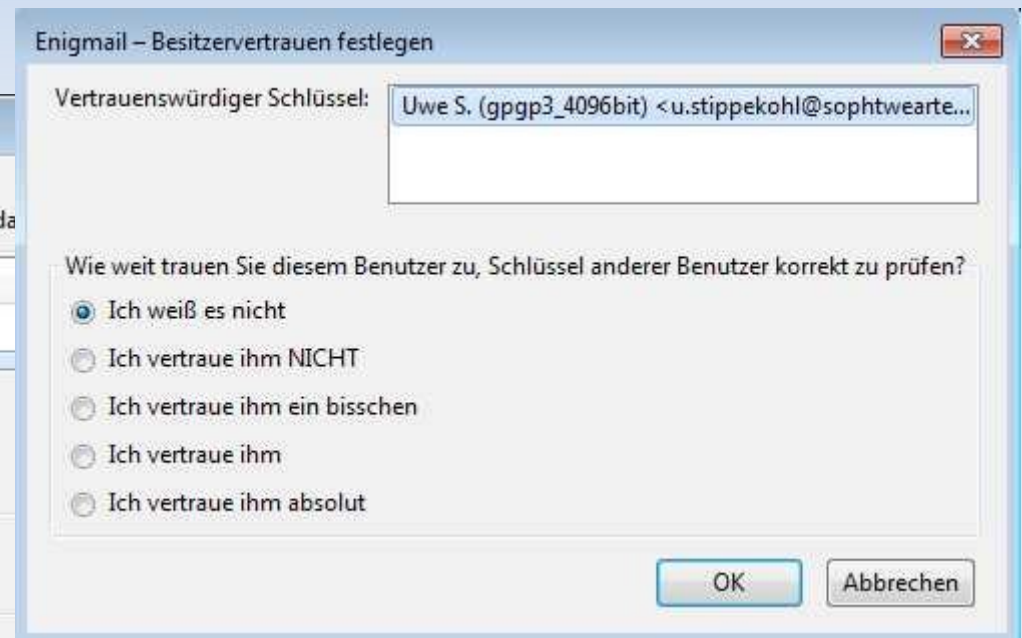
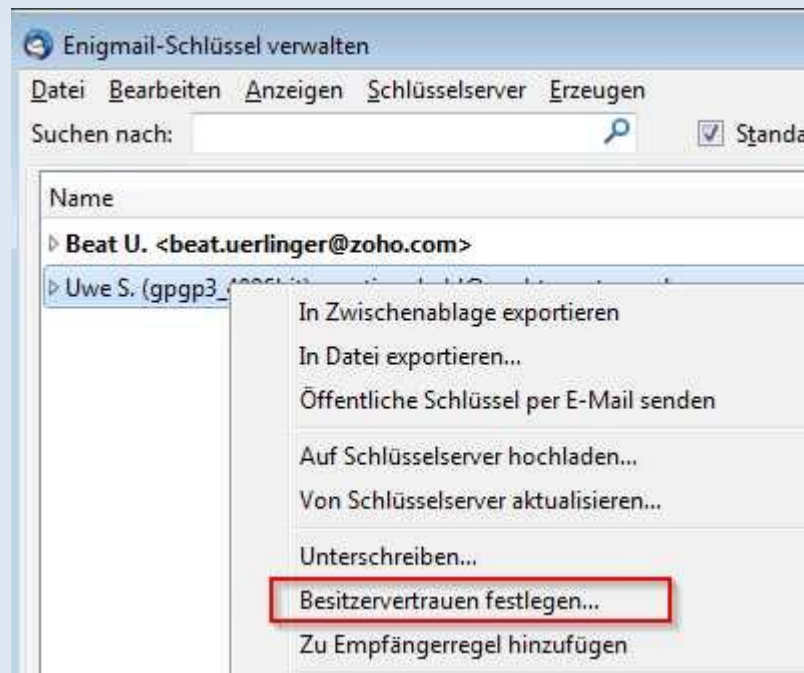




Workshop: Emailverschlüsselung

Schlüsselverwaltung

- Vertrauen festlegen
 - Unvertrauter Schlüssel
 - Volles Vertrauen



Workshop: Emailverschlüsselung



Anwendung

- Mail verschlüsseln

Verfassen: Paragraph zehn

Senden Rechtschr. Anhang S/MIME Speichern

Enigma!:

Von: Beat U. <beat.uerlinger@zoho.com> beat.uerlinger@zoho.com

An: u.stippekoehl@sophwareteam.de

Betreff: Paragraph zehn

Das Briefgeheimnis ist ein in der Verfassung demokratischer Staaten garantiertes Grundrecht, das die Unverletzlichkeit von Briefen garantiert. Abzugrenzen ist es vom Postgeheimnis und dem Fernmeldegeheimnis, welchem der Schutz elektronischer Kommunikation unterliegt.

In der Bundesrepublik De des Grundgesetzes garant dabei jede schriftliche Empfänger zu verstehen. verschlossenen Sendungen Einschränkungen des Brie Gesetzesvorbehalt (Artik Geheimdiensten, Strafpro

Eine Beschlagnahmung von dürfen verschlossene Pos Polizei oder dem Staatsa (§ 100 Abs. 3 S. 4 StPO) Beschlagnahme von Postse Postunternehmens befinden.

Bestraft wird eine Verletzung des Briefgeheimnisses gem. § 202 StGB. Das Briefgeheimnis umfasst hierbei jedes Schriftstück, das verschlossen bzw. durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist.

Enigma!-Sendeoptionen

- Nachricht verschlüsseln
- Nachricht unterschreiben
- Inline-PGP verwenden
- PGP/MIME verwenden

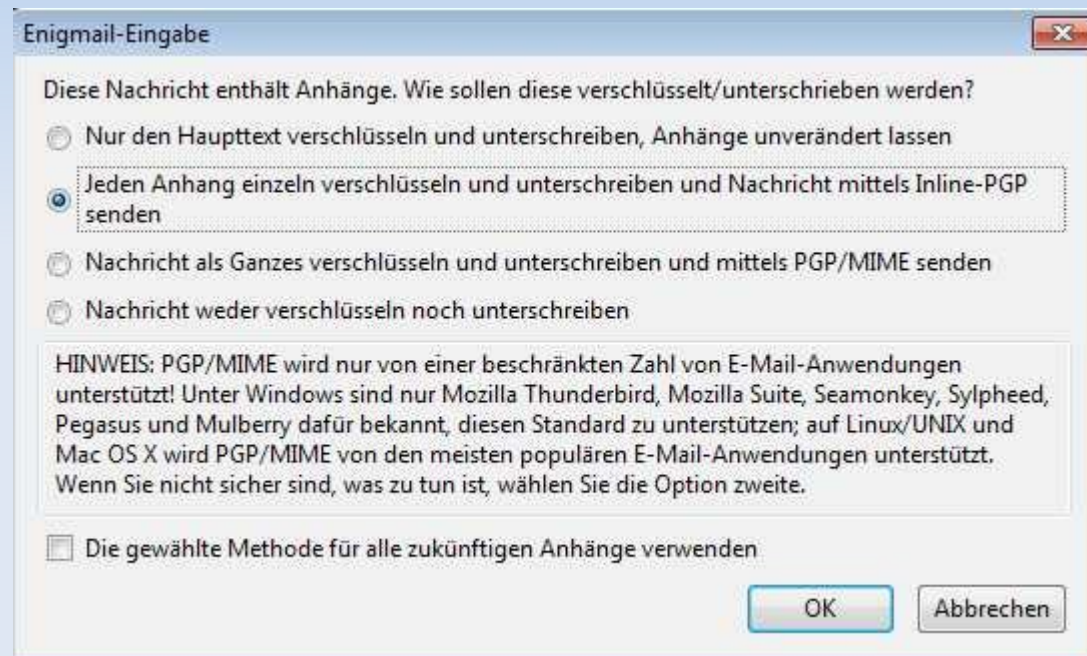
OK Standardwerte wieder herstellen Abbrechen

Workshop: Emailverschlüsselung



Anwendung

- Mail verschlüsseln

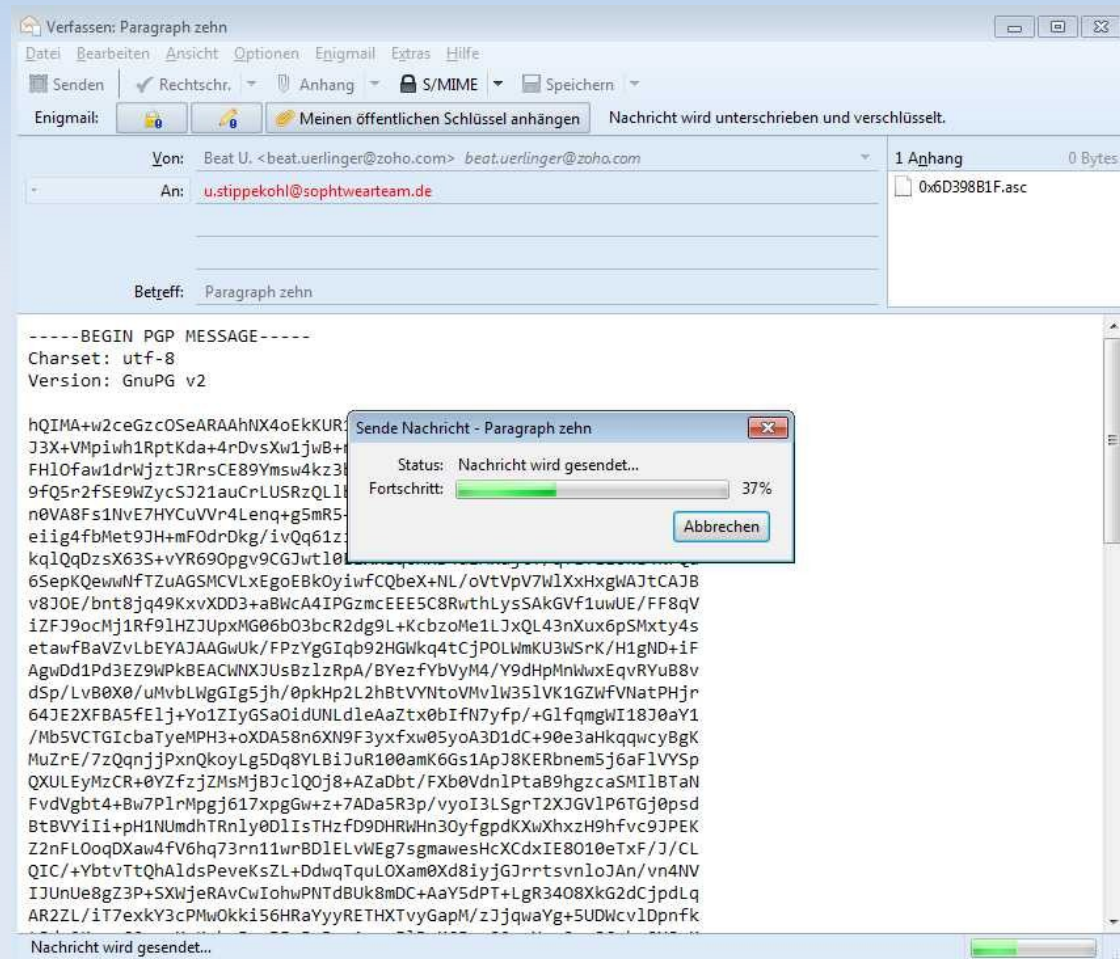


Workshop: Emailverschlüsselung



Anwendung

- Mail verschlüsseln



Workshop: Emailverschlüsselung



Anwendung

- Mail entschlüsseln

The screenshot shows a mail client interface with a message from 'beat.uerlinger@zoho.com' titled 'Paraglyph zehn' addressed to 'u.stippekoehl@sophtwearteam.de'. The message body contains a PGP-encrypted block starting with '-----BEGIN PGP MESSAGE-----'. A 'Pinentry' dialog box is overlaid on the message, displaying a blue key icon and the following text: 'Sie benötigen eine Passphrase, um den geheimen OpenPGP Schlüssel zu entsperren. Benutzer: "Beat U. <beat.uerlinger@zoho.com>" 4096-bit RSA Schlüssel, ID 467D58F9, erzeugt 2016-01-07 (HauptschlüsselID 6D398B1F)'. Below the text is a text input field for the password and 'OK' and 'Cancel' buttons.

Workshop: Emailverschlüsselung



Anwendung

- Mail entschlüsseln

The screenshot shows an email client interface. At the top, there are action buttons: 'Antworten', 'Weiterleiten', 'Archivieren', 'Junk', 'Löschen', and 'Mehr'. The email header shows 'Von Mir', 'Betreff Paragraph zehn', and 'An u.stippekoehl@sophtwearteam.de'. The main content area shows an 'Enigmail' message with the subject 'Entschlüsselte Nachricht; Korrekte Unterschrift von Beat U. <beat.uerlinger@zoho.com>'. The message text discusses the right to privacy in Germany. A context menu is open over the message, listing options like 'Enigmail-Sicherheitsinfo...', 'Schlüsseleigenschaften anzeigen', and 'Schlüssel unterschreiben...'. At the bottom, there is an attachment '1 Anhang: 0x6D398B1F.asc.pgp 4,2 KB' and a 'Speichern' button.

Workshop: Emailverschlüsselung



Datensicherung f. Thunderbird (Windows)

- Thunderbird beenden!
- Windows-Explorer öffnen



Workshop: Emailverschlüsselung



Datensicherung f. Thunderbird (LINUX)

- Thunderbird beenden!
- Dateimanager (STRG +H), re. MT auf .thunderbird

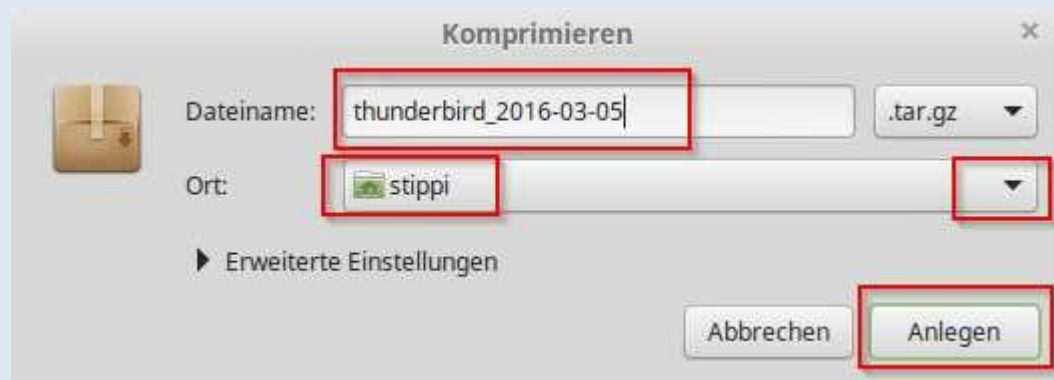


Workshop: Emailverschlüsselung



Datensicherung f. Thunderbird (LINUX)

- Dateinamen vergeben (Wichtig!) führenden Punkt entfernen!
- Dateiendung wählen, Ort (Ordner) wählen (USB-Medium?)
- Am Ende STRG + H um wieder versteckte Dateien / Ordner zu verstecken



Workshop: Emailverschlüsselung



Quellen:

- <https://www.thunderbird-mail.de/lexicon/entry/17-enigmail/>
- <http://www.kryptowissen.de/enigmail-thunderbird-windows-tutorial.html>
- <http://www.german-privacy-fund.de/tutorial-e-mails-verschluseln-in-30-minuten-alternative-2/>
-



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.