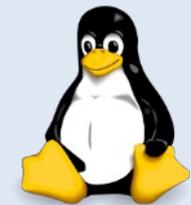


Workshop: Email-Verschlüsselung



Tagesordnungspunkte

- Begrüßung und Einführung
- 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

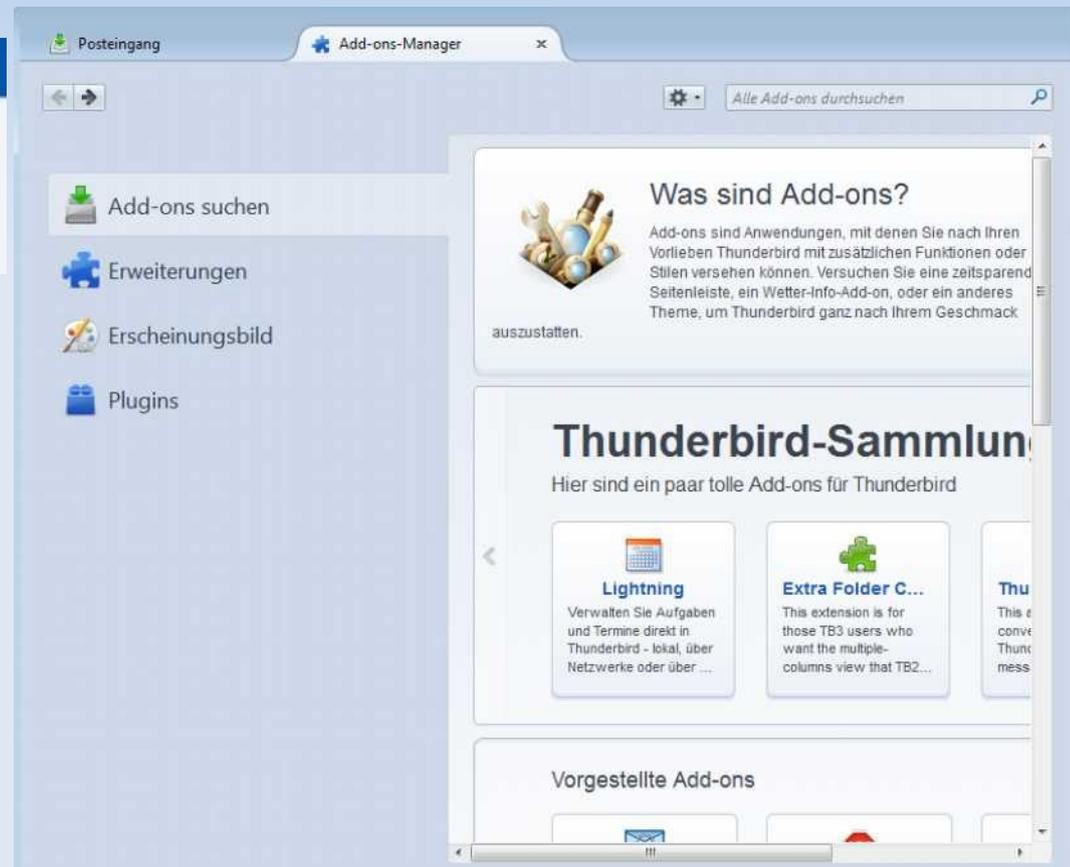
- Asymmetrische Verschlüsselung
- Public-Key-Verfahren
- Besteht aus einem privaten und einem öffentlichen Schlüssel
- Privater Schlüssel bleibt immer bei mir! (Sicherung!)
- Öffentlicher Schlüssel als Datei, auf Schlüsselservers oder Text
- Verschlüsselung mit öffentlichem Schlüssel
- Entschlüsselung mit privatem Schlüssel
 - Passphrase vs. Kennwort (Länge)
 - z. B. #Ich_fühl_mich_\$icher_mit_Verschlüsselung

Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on)



Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on)

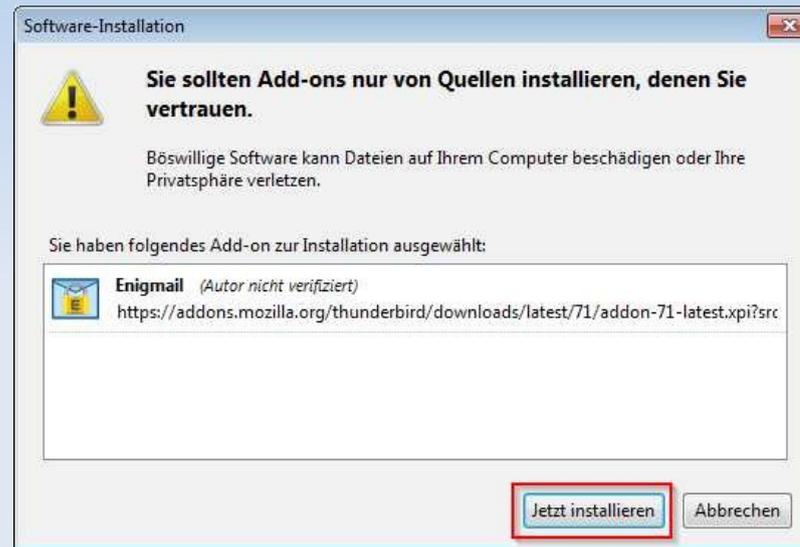
A screenshot of the Enigmail 1.8.2 add-on page for Thunderbird. The page features a blue header with the Enigmail logo (a yellow envelope with a blue 'E') and the text 'Enigmail 1.8.2 von Patrick Brunschwig'. Below this, a description reads 'Verschlüsseln und Authentifizieren von Nachrichten mit OpenPGP. Benötigt...' (partially visible). A prominent green button with a white plus sign and the text 'Zu Thunderbird hinzufügen' is highlighted with a red rectangular 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, there are two rows of statistics: 'Bewertung' with a 4.5-star rating and '184 Bewertungen', and 'Aktive Nutzer' with the number '140.744'.

Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on)

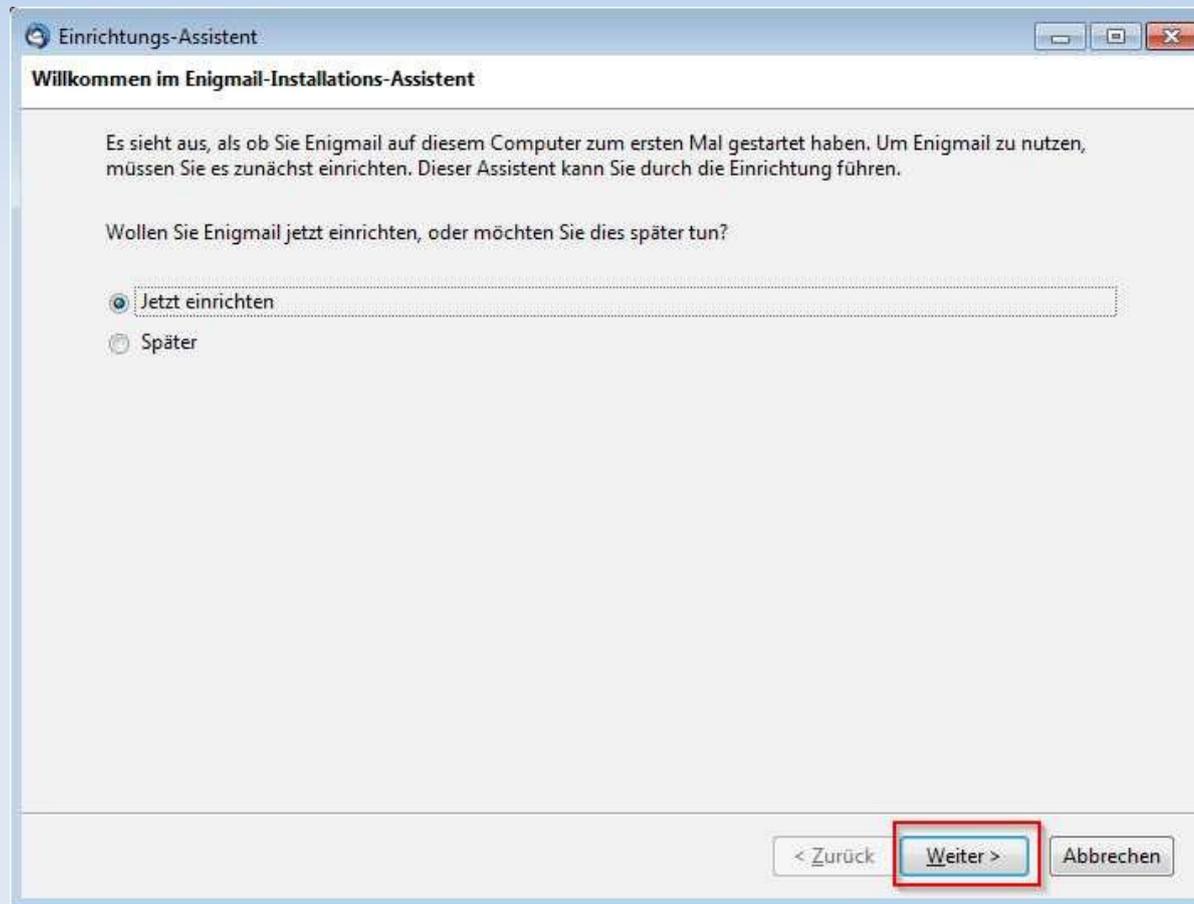


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail

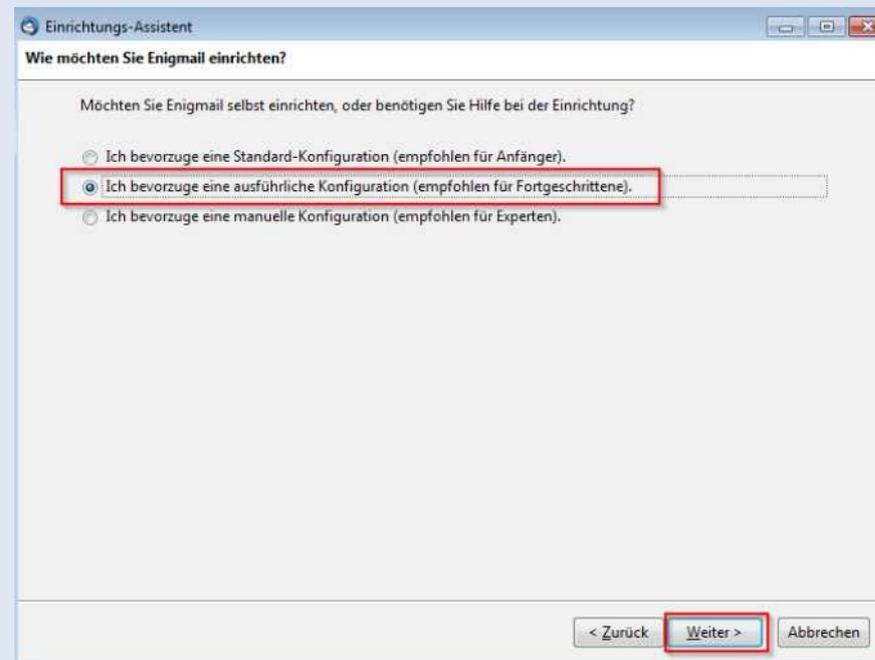


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

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

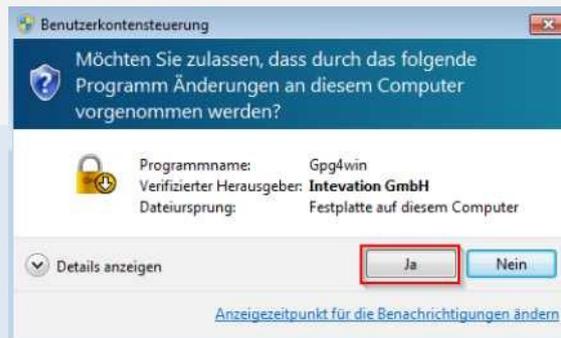
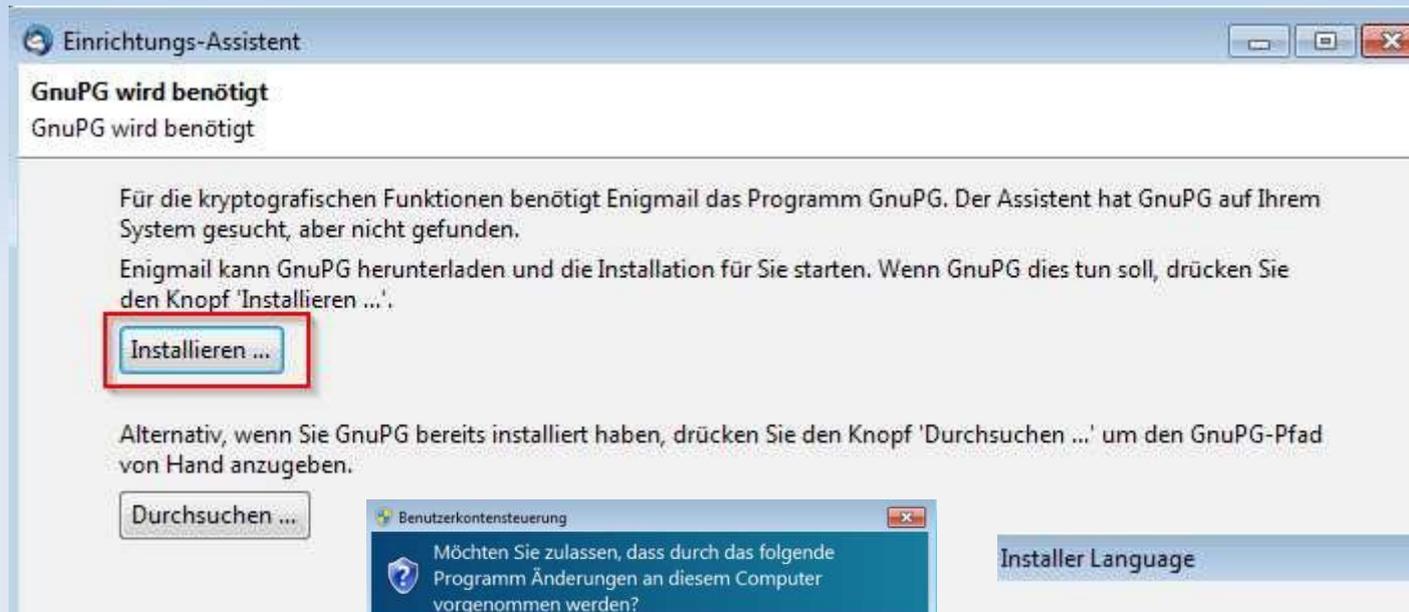


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG



Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG



Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG



Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG



Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG



Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG



Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- GnuPG

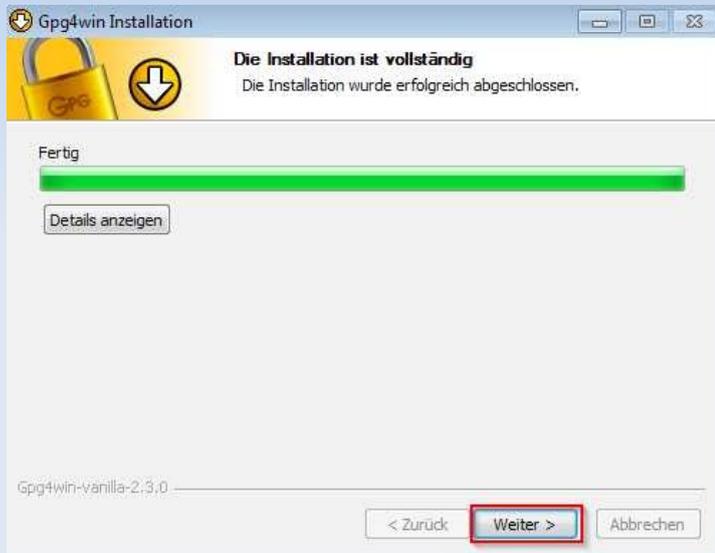




Workshop: Emailverschlüsselung

Einrichtungs-Assistent

- GnuPG

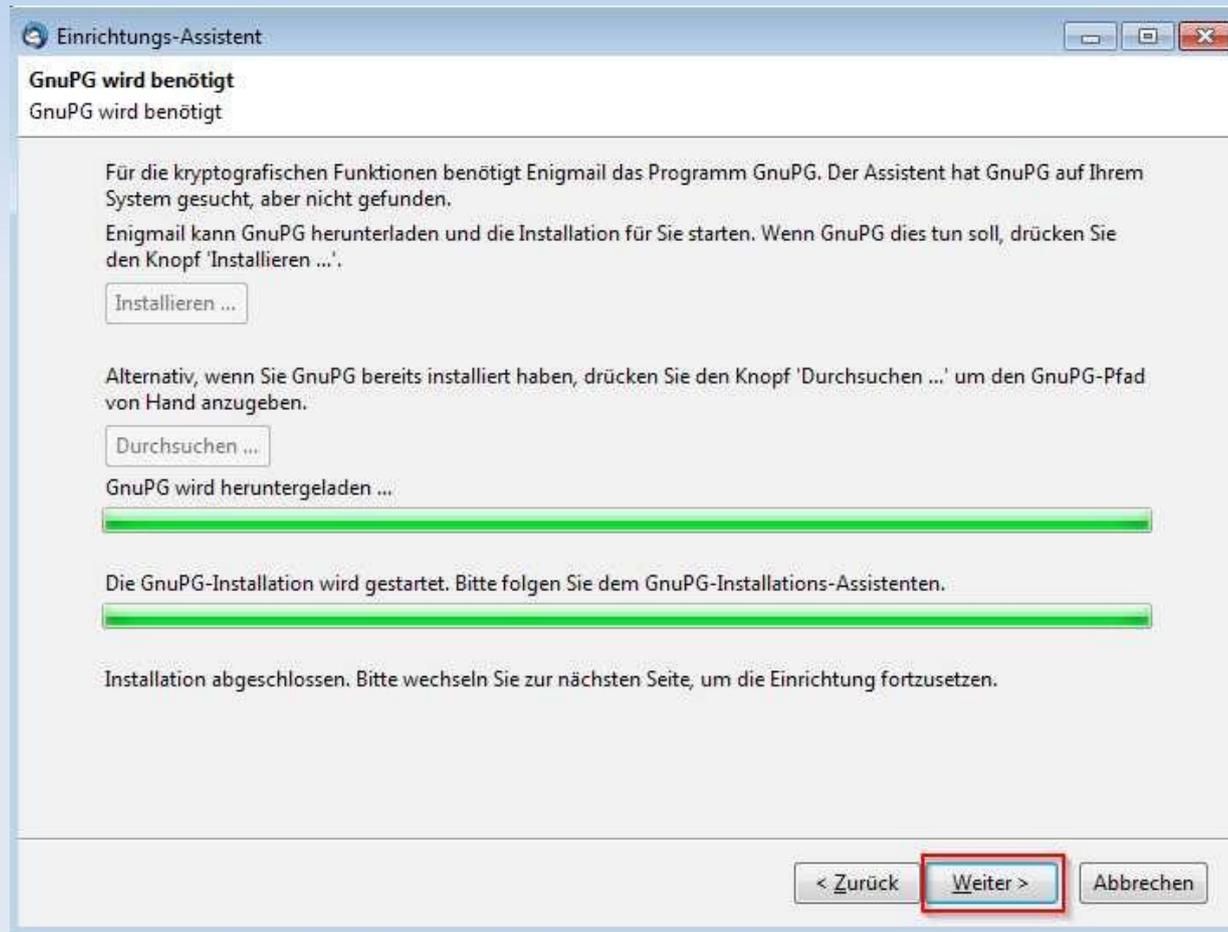




Workshop: Emailverschlüsselung

Einrichtungs-Assistent

- Enigmail (Fortsetzung)

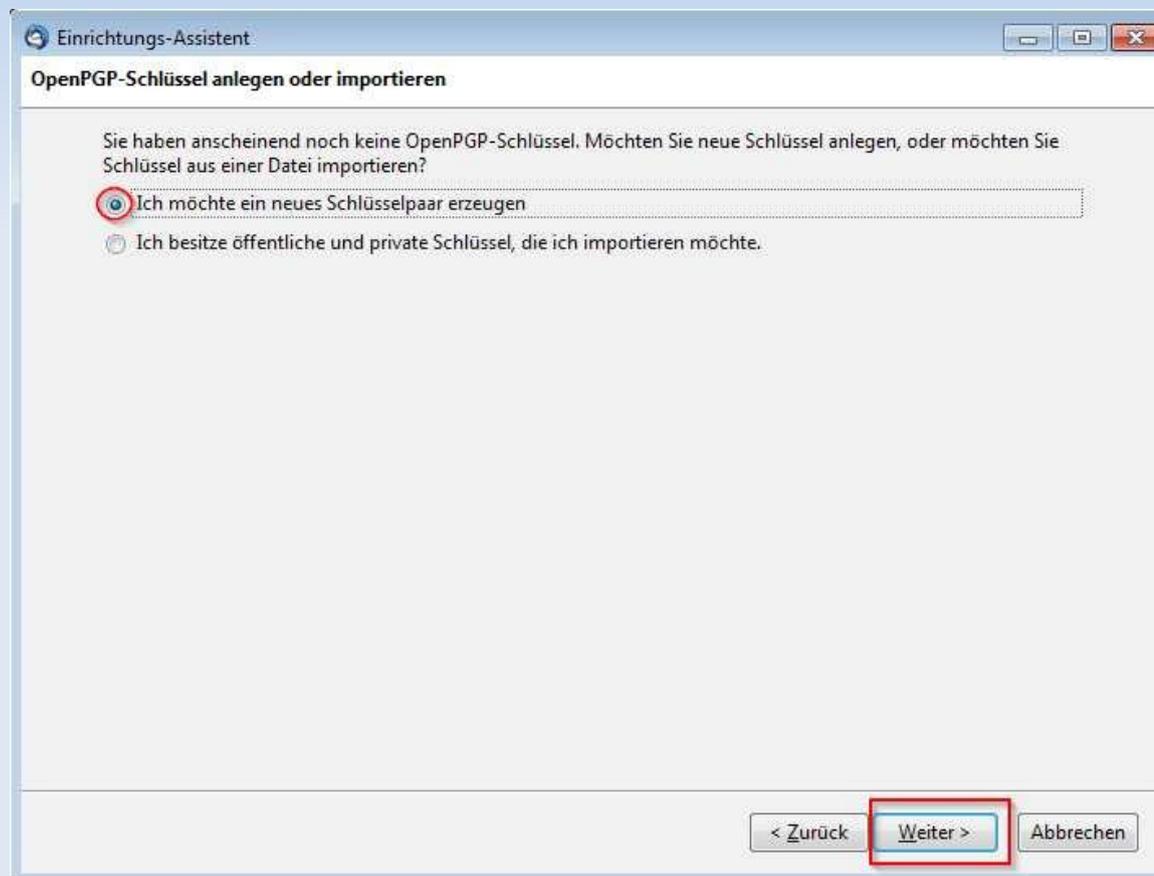


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)

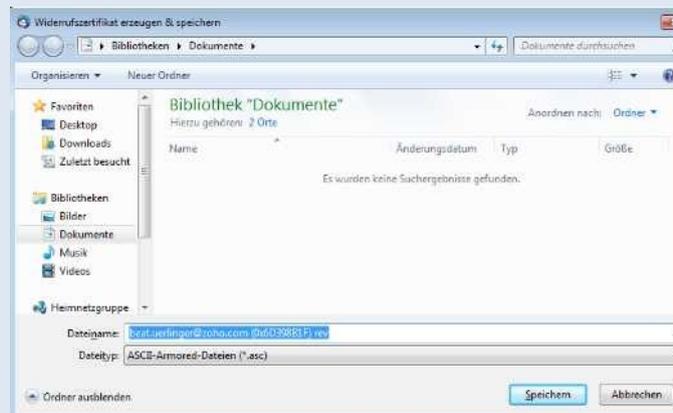
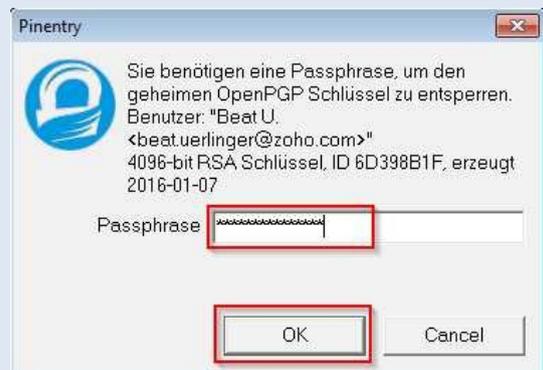
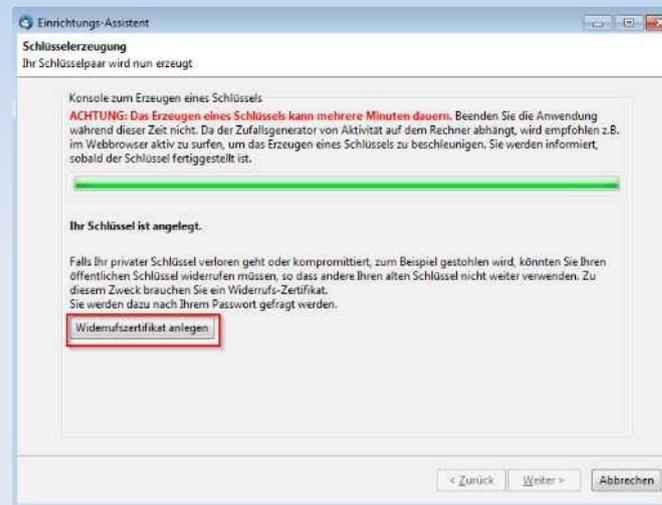
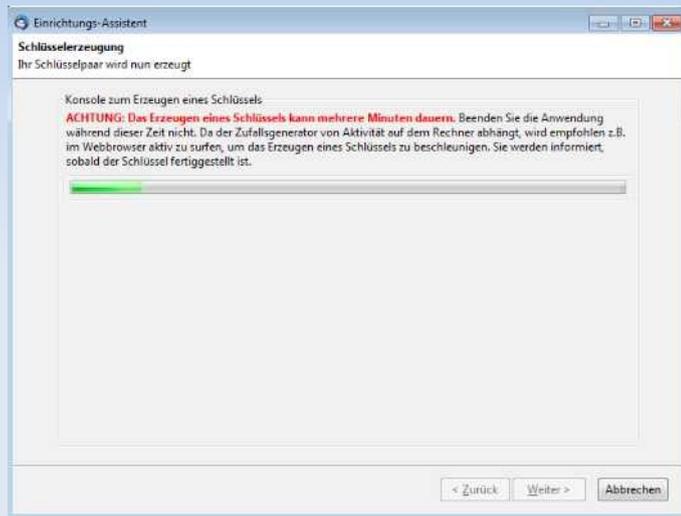


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)

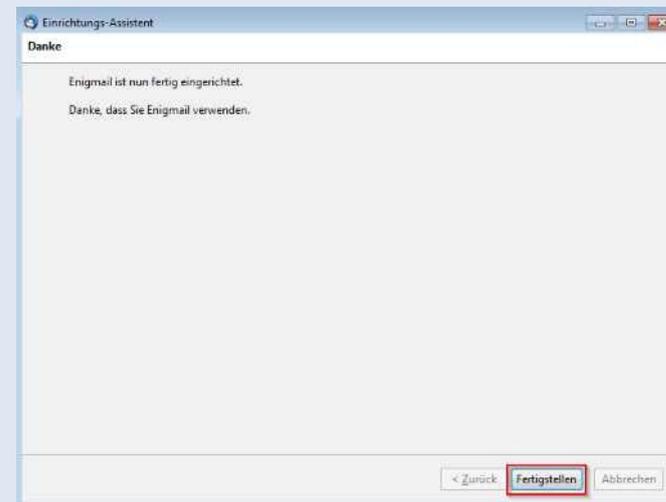
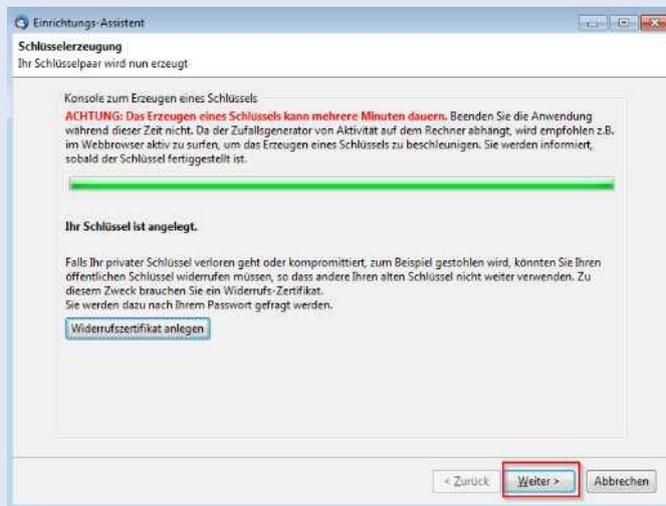
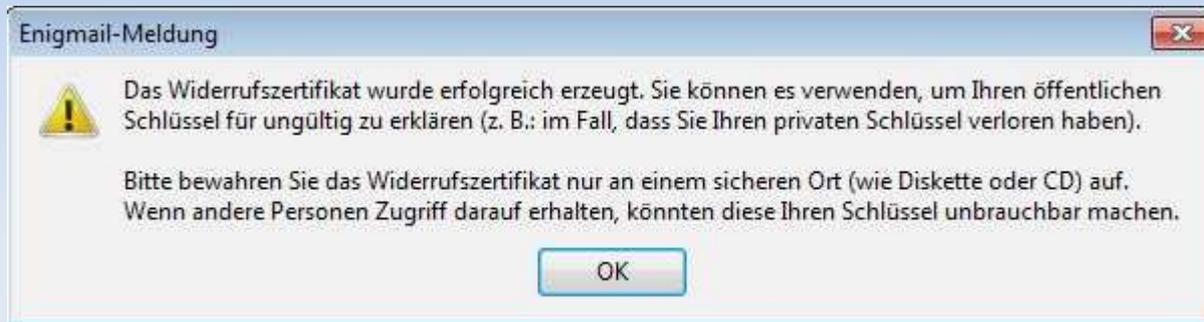


Workshop: Emailverschlüsselung



Einrichtungs-Assistent

- Enigmail (Fortsetzung)

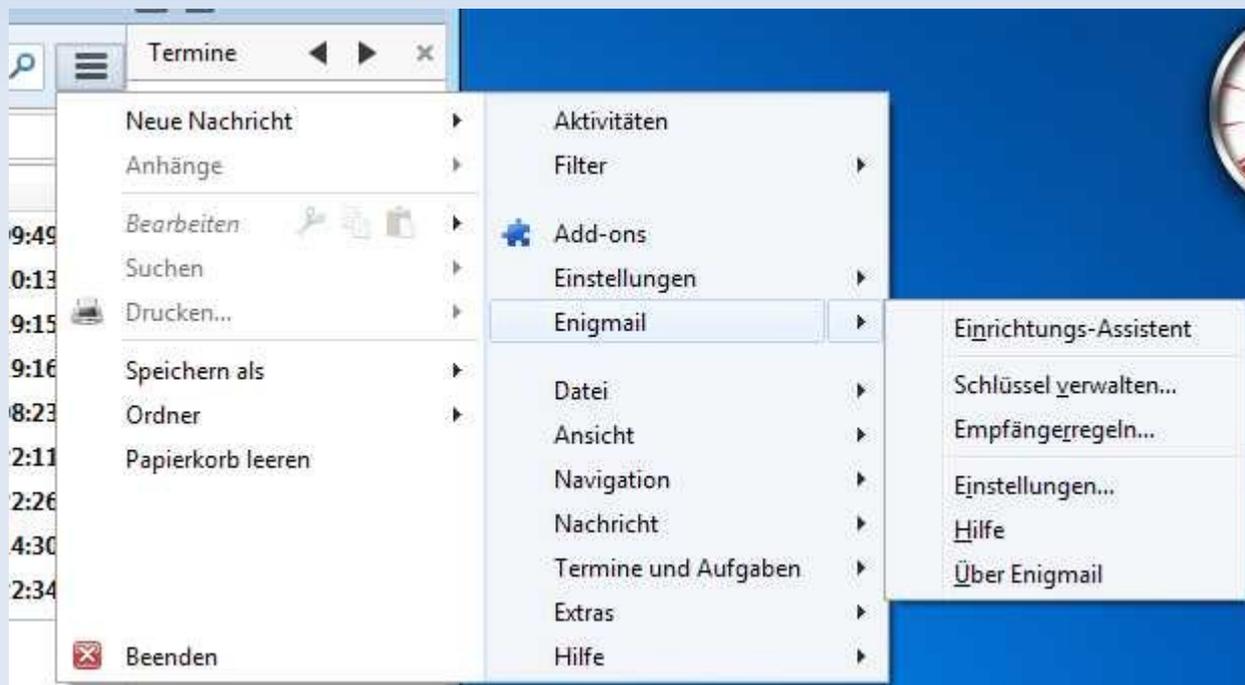


Workshop: Emailverschlüsselung



Installation

- Enigmail (Add-on) benutzen

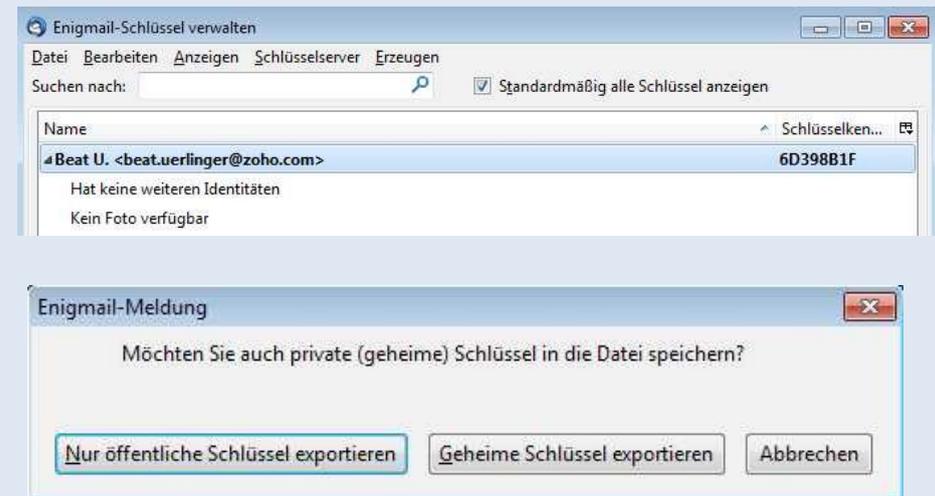
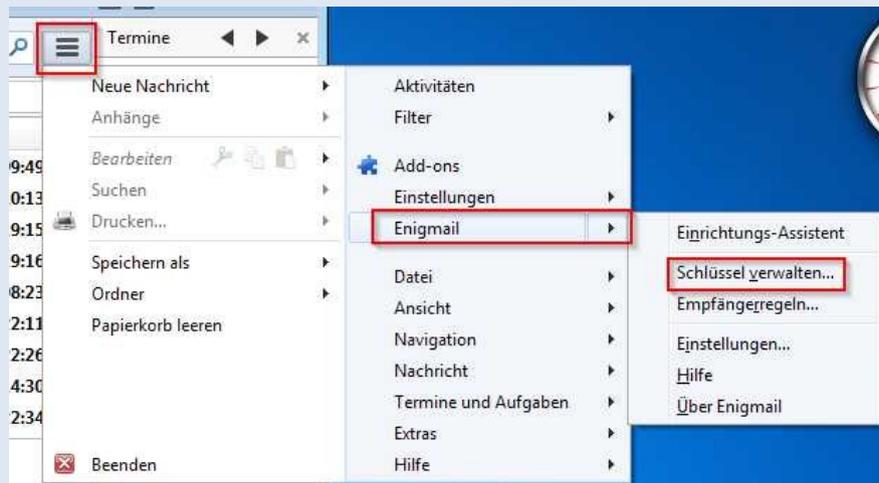


Workshop: Emailverschlüsselung



Schlüsselverwaltung

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

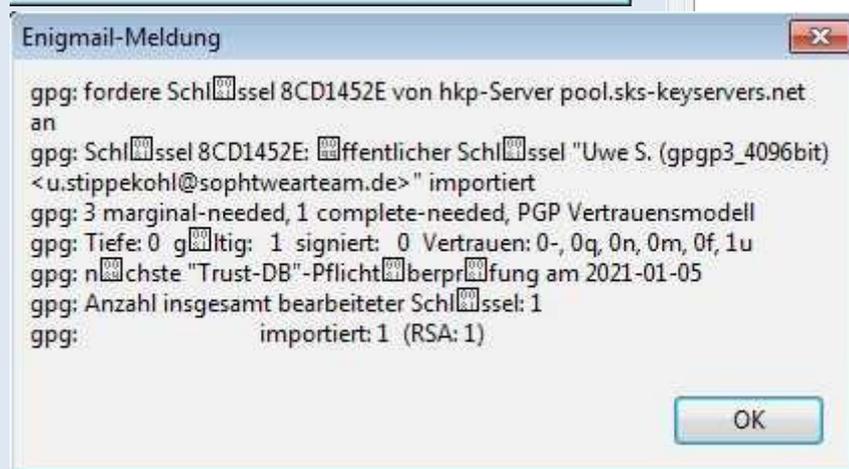
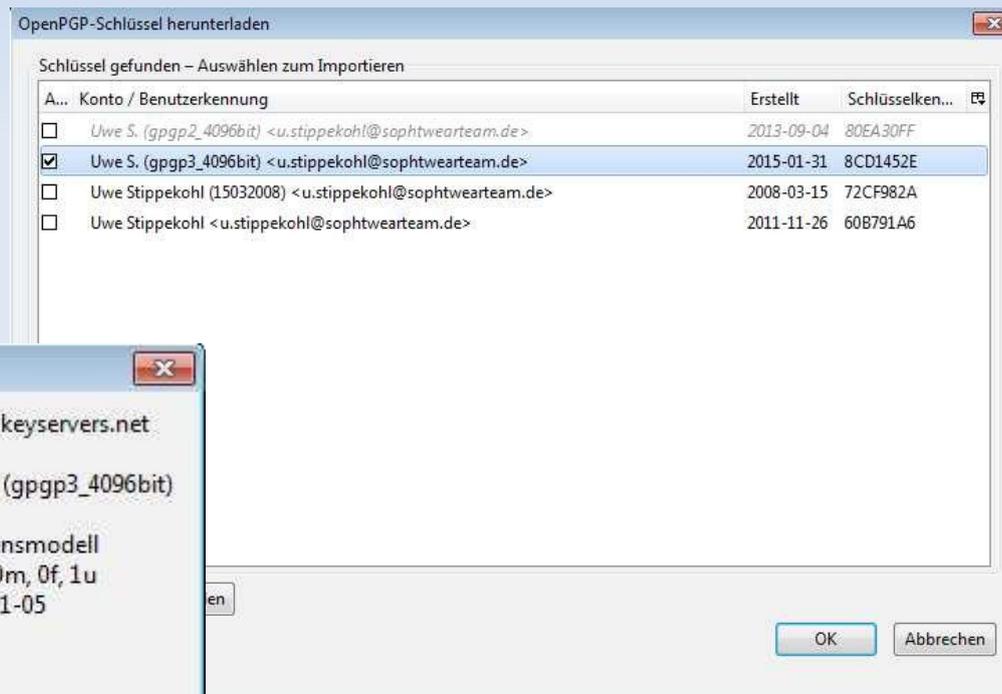


Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel importieren
 - Fremde Schlüssel importieren

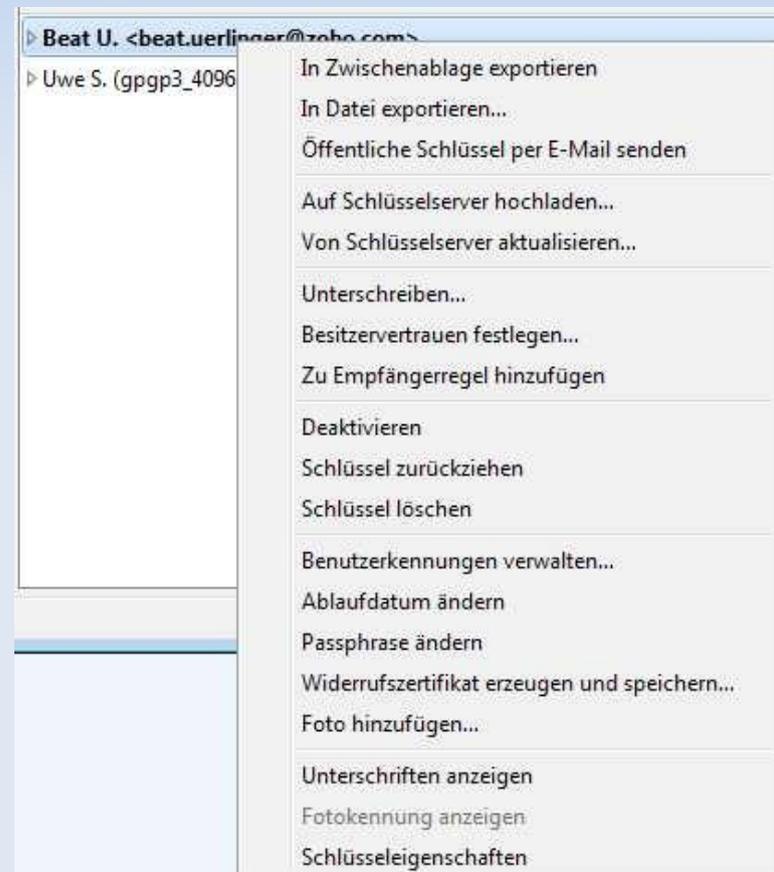


Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel exportieren
 - Eigenen Schlüssel exportieren oder sichern

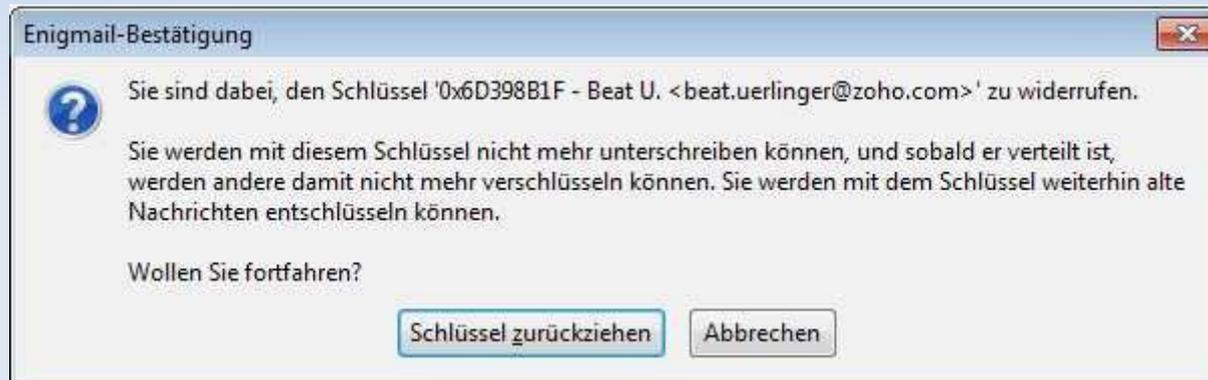


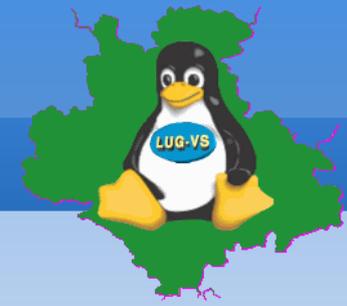
Workshop: Emailverschlüsselung



Schlüsselverwaltung

- Schlüssel importieren, exportieren, sichern
 - Widerrufszeugnis anwenden, Schlüssel zurückziehen

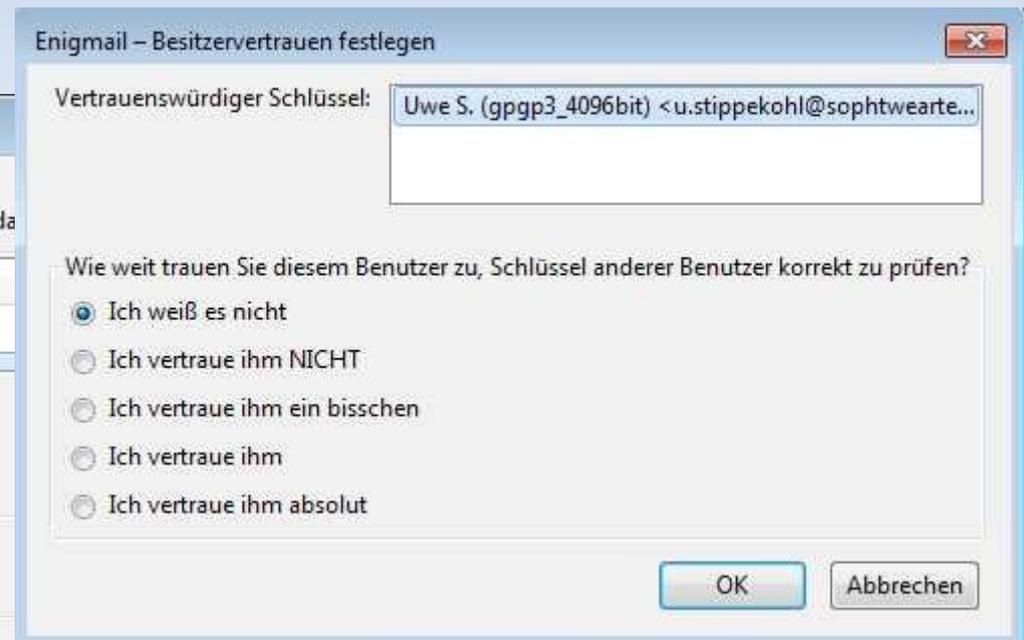
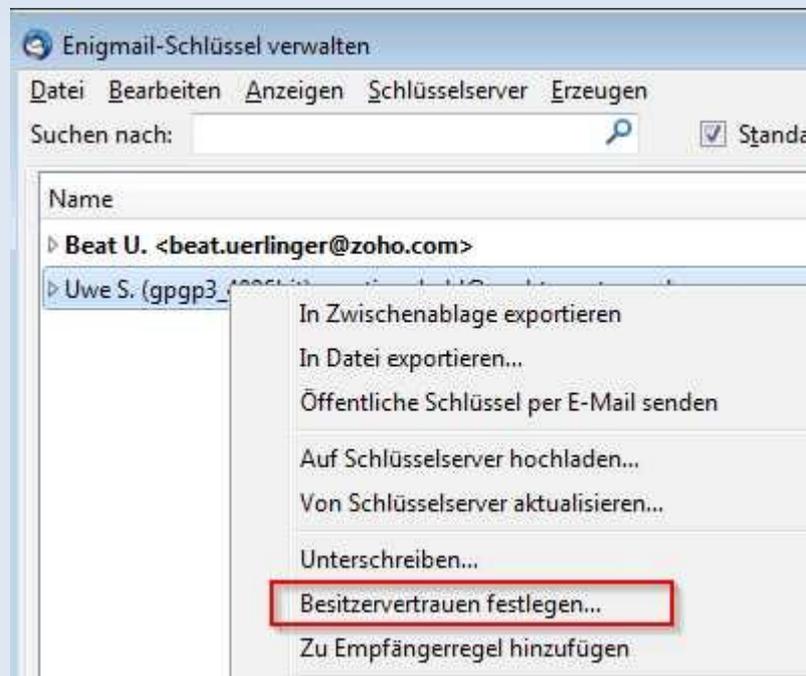




Workshop: Emailverschlüsselung

Schlüsselverwaltung

- Vertrauen festlegen
 - Unvertrauter Schlüssel
 - Volles Vertrauen



Workshop: Emailverschlüsselung



Anwendung

- Mail verschlüsseln

The screenshot shows the 'Verfassen: Paragraph zehn' window in an email client. The 'Enigma' dialog box is open, displaying the following options:

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

Buttons at the bottom of the dialog include 'OK', 'Standardwerte wieder herstellen', and 'Abbrechen'.

The background text in the email editor includes:

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.

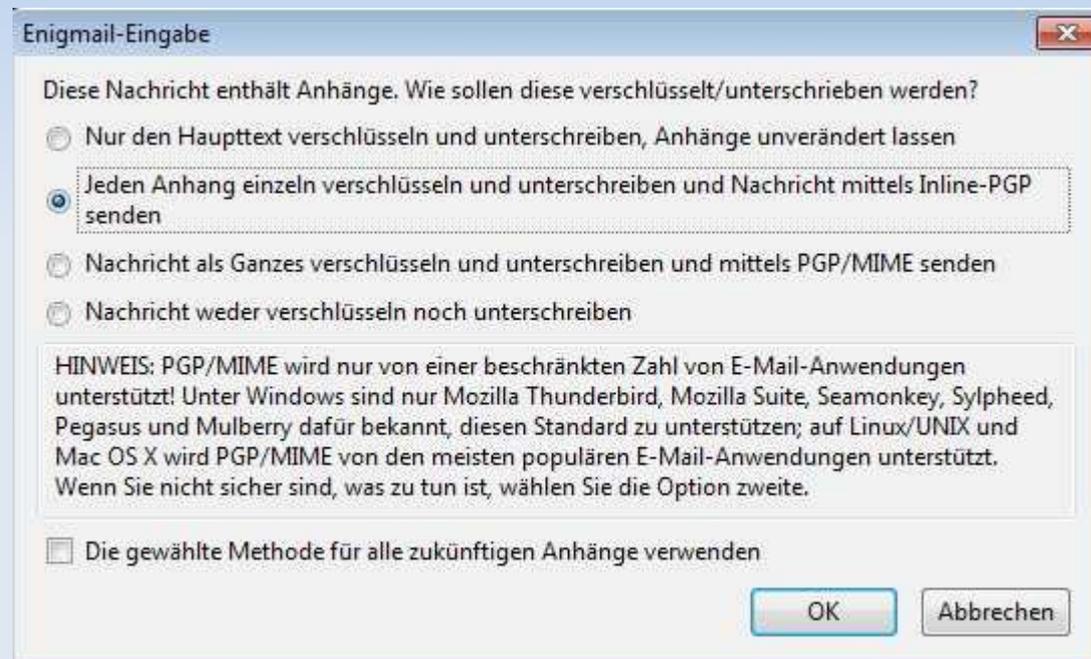
Bestraft wird eine Verletzung des Briefgeheimnisses gem. § 202 StGB. Das Briefgeheimnis umfasst hierbei jedes Schriftstück, das verschlossen bzw. durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist.

Workshop: Emailverschlüsselung



Anwendung

- Mail verschlüsseln



Workshop: Emailverschlüsselung



Anwendung

- Mail verschlüsseln

The screenshot shows an email client window titled "Verfassen: Paragraph zehn". The interface includes a menu bar with "Datei", "Bearbeiten", "Ansicht", "Optionen", "Enigmail", "Extras", and "Hilfe". Below the menu is a toolbar with buttons for "Senden", "Rechtschr.", "Anhang", "S/MIME", and "Speichern". The "Enigmail" section shows a status bar indicating "Nachricht wird unterschrieben und verschlüsselt." and a button for "Meinen öffentlichen Schlüssel anhängen".

The email header shows the sender as "Beat U. <beat.uerlinger@zoho.com>" and the recipient as "u.stippekoehl@sophtwearteam.de". The subject is "Paragraph zehn". An attachment named "0x6D398B1F.asc" is visible in the right pane.

The main content area displays a PGP message header: "-----BEGIN PGP MESSAGE-----", "Charset: utf-8", and "Version: GnuPG v2". Below this is a long block of Base64-encoded text representing the encrypted message content.

A small dialog box titled "Sende Nachricht - Paragraph zehn" is overlaid on the message content. It shows the status "Nachricht wird gesendet..." and a progress bar at 37%. There is an "Abbrechen" button.

At the bottom of the window, a status bar indicates "Nachricht wird gesendet..." with a green progress indicator.

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, requesting a password to decrypt the message. The dialog text reads: '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)'. There is an empty text 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 displays 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 democratic states and Germany's Basic Law. 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



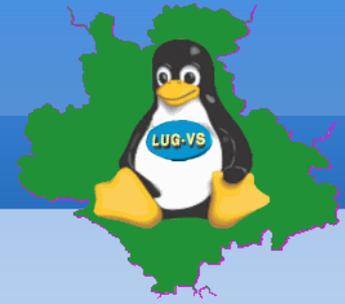
Workshop: Emailverschlüsselung



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.