

# Verschlüsselung

**Linux im Alltag 2019 – VHS Mülheim**

# Was haben wir vor?

- Motivation
- Wie funktioniert Verschlüsselung?
- Wie funktioniert Email-Verschlüsselung?
- Welche Verfahren gibt es?
- S/MIME – Wie geht es konkret?
- PGP – Wie geht es konkret?

# Warum verschlüsseln?

- Emails sind ohne Verschlüsselung wie Postkarten – jeder, an dem sie vorbeikommen, kann einen Blick darauf werfen
- Oder sogar schlimmer: Inhalte verändern und der Empfänger bekommt andere oder weniger Informationen
- Insgesamt soll der Inhalt der Kommunikation nicht in falsche Hände geraten

## Ziele:

- Integrität
- Vertraulichkeit

# Was hätten wir gerne?

- Integrität  
keine Verfälschung von Inhalten
- Vertraulichkeit  
nur der gewünschte Empfänger darf Inhalt lesen
- Authentizität  
Die Inhalte kommen tatsächlich von dem Absender, der in der Email steht
- Das alles bei möglichst wenig Zusatzaufwand

# Status Quo bei Email

- Analogie zur Postkarte
- Inhalte können unbemerkt mitgelesen werden
- Inhalte können verfälscht werden
- Absender kann vorgetäuscht werden

# Wie funktioniert Verschlüsselung?

- Verschlüsselung wandelt lesbaren Klartext in nicht interpretierbare Zeichenfolge um
- Parameter:
  - Ein oder mehrere Schlüssel
  - Verschlüsselungsverfahren

# Asymmetrische Verschlüsselung

# Asymmetrische Verschlüsselung

**Bernd**

# Asymmetrische Verschlüsselung

**Bernd**

---

**Anja**

# Asymmetrische Verschlüsselung

**Bernd**

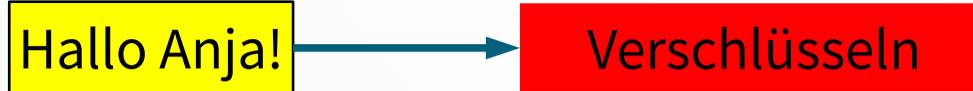
Hallo Anja!

---

**Anja**

# Asymmetrische Verschlüsselung

**Bernd**



---

**Anja**

# Asymmetrische Verschlüsselung

**Bernd**

Hallo Anja!



Verschlüsseln

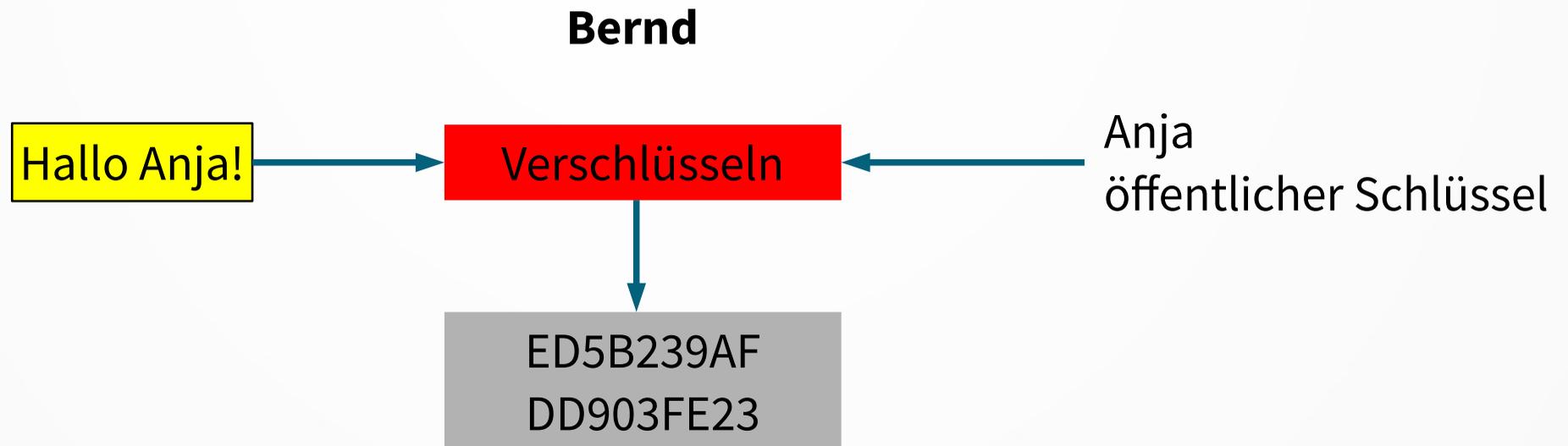


Anja  
öffentlicher Schlüssel

---

**Anja**

# Asymmetrische Verschlüsselung



**Anja**

# Asymmetrische Verschlüsselung

**Bernd**

Hallo Anja!

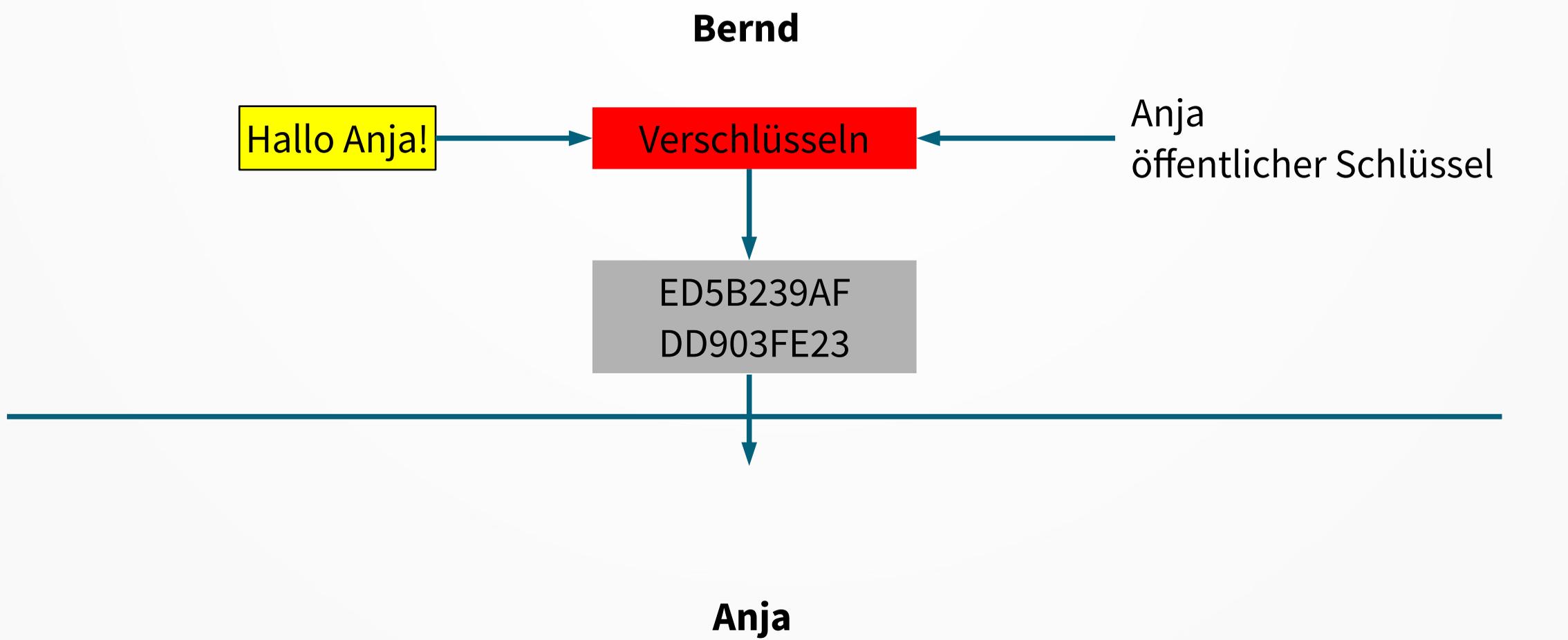
Verschlüsseln

Anja  
öffentlicher Schlüssel

ED5B239AF  
DD903FE23

---

**Anja**



# Asymmetrische Verschlüsselung

**Bernd**

Hallo Anja!

Verschlüsseln

Anja  
öffentlicher Schlüssel

ED5B239AF  
DD903FE23

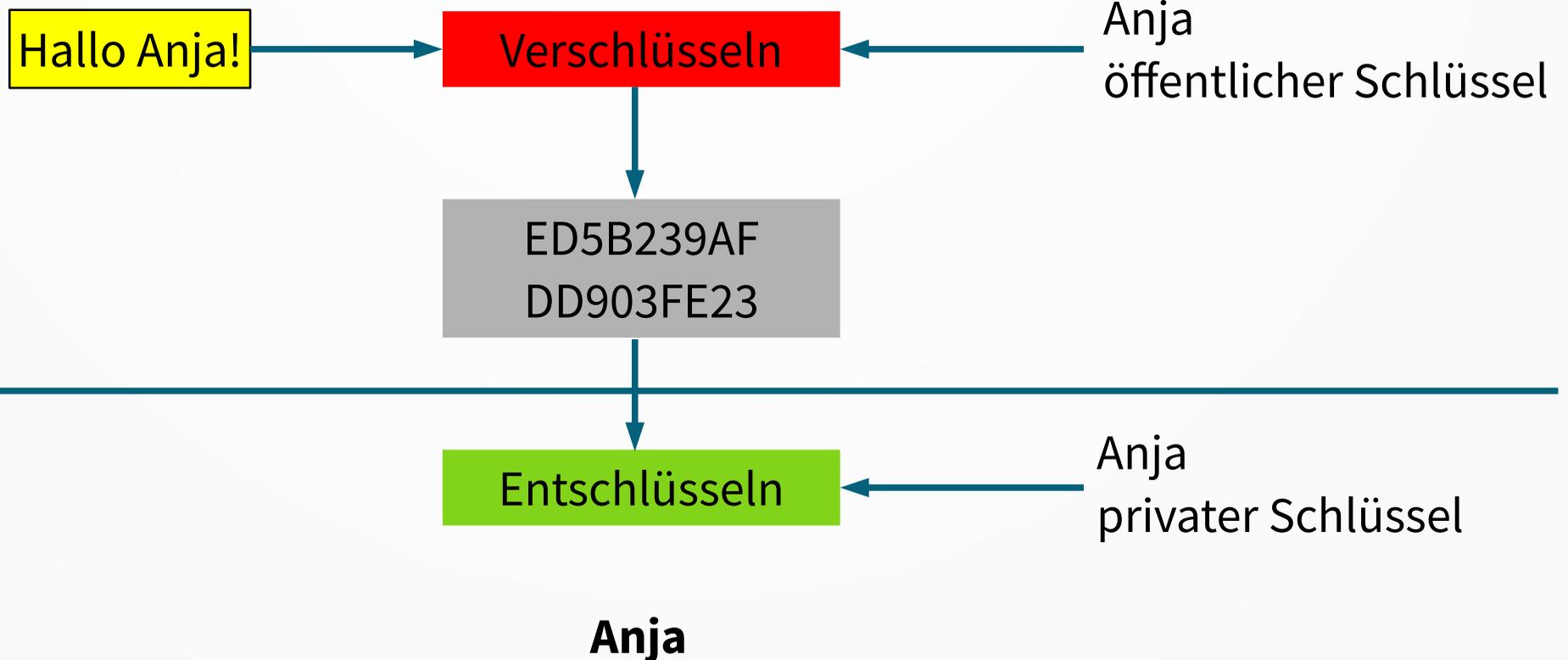
Entschlüsseln

**Anja**



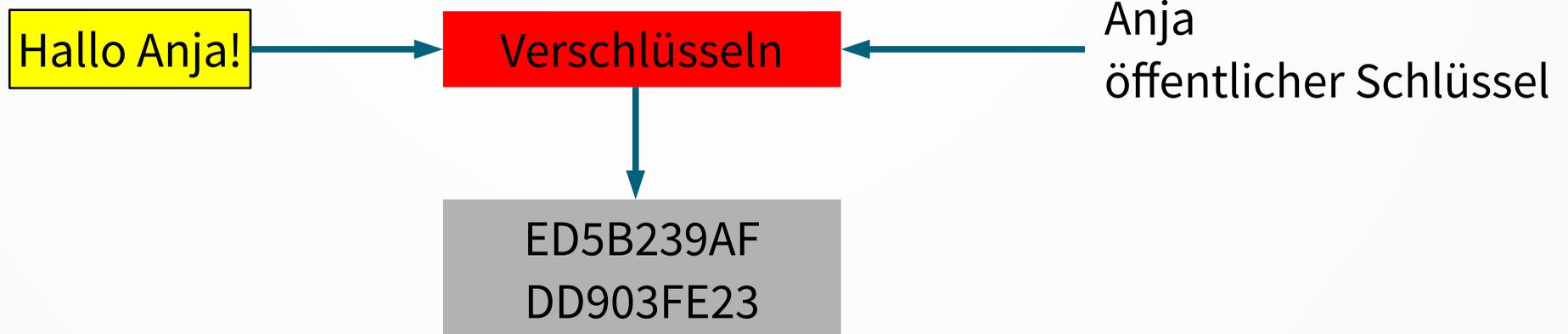
# Asymmetrische Verschlüsselung

**Bernd**



# Asymmetrische Verschlüsselung

**Bernd**



**Anja**

# Asymmetrische Verschlüsselung

- Anja benötigt ein Schlüsselpaar aus öffentlichem und privatem Schlüssel
- Bernd muss den öffentlichen Schlüssel von Anja haben
- Bernd muss sich sicher sein, dass er auch wirklich Anjas öffentlichen Schlüssel hat und nicht Eva, die sich für Anja ausgibt
- Anja muss auf ihren privaten Schlüssel aufpassen, da jeder, der diesen hat, Inhalte an sie lesen kann

# Anja benötigt ein Schlüsselpaar

- Zusammengehörige Schlüsselpaare kann man auf dem Rechner mit Zufallszahlen erstellen.
- Lokal auf dem Rechner erstellen, da sonst der private Schlüssel schon irgendwo anders als auf dem eigenen Rechner war → nicht mehr privat

# Bernd muss den öffentlichen Schlüssel von Anja haben

- Bernd schickt Anja eine Email mit dem öffentlichen Schlüssel
- Bernd lädt seinen öffentlichen Schlüssel auf sog. Keyserver hoch und Anja lädt ihn von dort herunter
- Öffentlicher Schlüssel darf/muss verteilt werden (wie der Name „öffentlich“ schon sagt)

# Bernd muss sich sicher sein, dass er den richtigen öffentlichen Schlüssel hat

- Es gibt Zertifizierungsstellen (Certificate Authorities, CAs), die überprüfen, ob öffentlicher Schlüssel zu einer Emailadresse gehört und falls ja, dies zertifizieren
- Emailprogramme vertrauen einer Liste an Zertifizierungsstellen
- Web of Trust  
Öffentliche Schlüssel werden von Benutzern durch direkten Schlüsselaustausch beglaubigt angesehen. Wenn der Schlüssel von einer Person meines Vertrauens beglaubigt wurde, vertraue ich dem auch
- Direkter Schlüsselaustausch mit Fingerprint

# Zertifizierungsstellen vs. Web of Trust

- Der Unterschied: Worauf basiert mein Vertrauen in den öffentlichen Schlüssel von Anja
- Zertifizierungsstellen: Dritte, denen Emailprogramme für diesen Zweck vertrauen und die Prüfung (üblicherweise) gegen Geld durchführen
  - Sectigo (ehem. Comodo): Ab 19,99 \$ pro Jahr
  - GlobalSign: Ab 59 \$ pro Jahr
  - SwissSign: Ab 39 CHF pro Jahr
- Web of Trust: Vertrauen wird durch beliebige andere vertrauenswürdige Personen hergestellt, zB Clara vertraut Anjas öffentlichem Schlüssel, Bernd vertraut Claras öffentlichem Schlüssel, dann vertraut Bernd über Clara auch Anjas öffentlichem Schlüssel

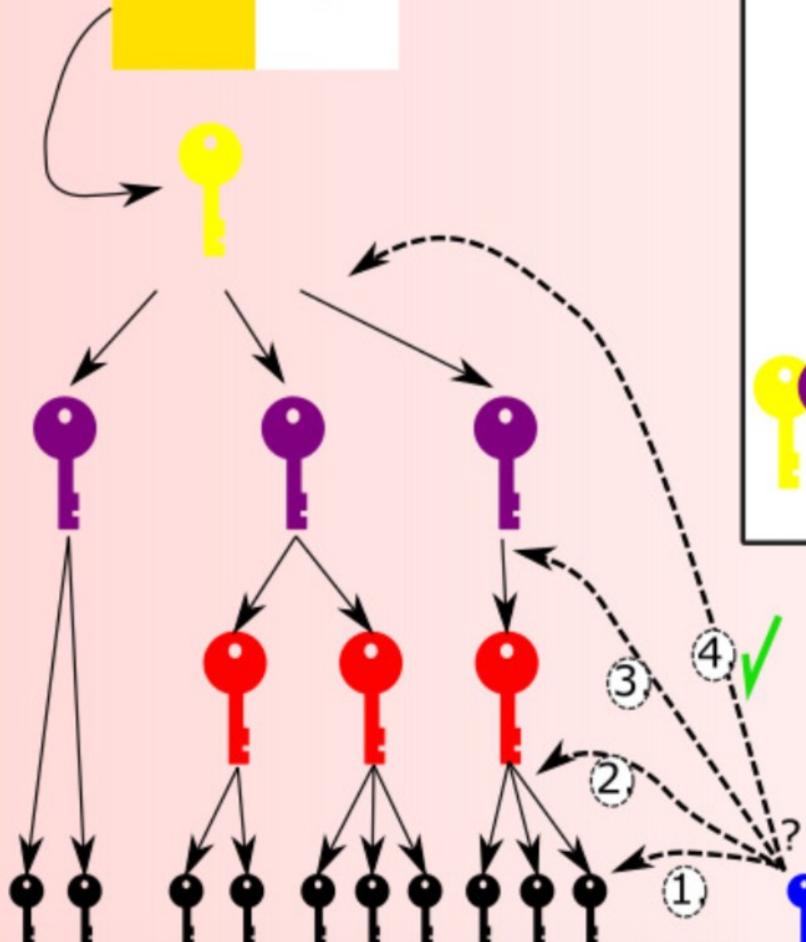
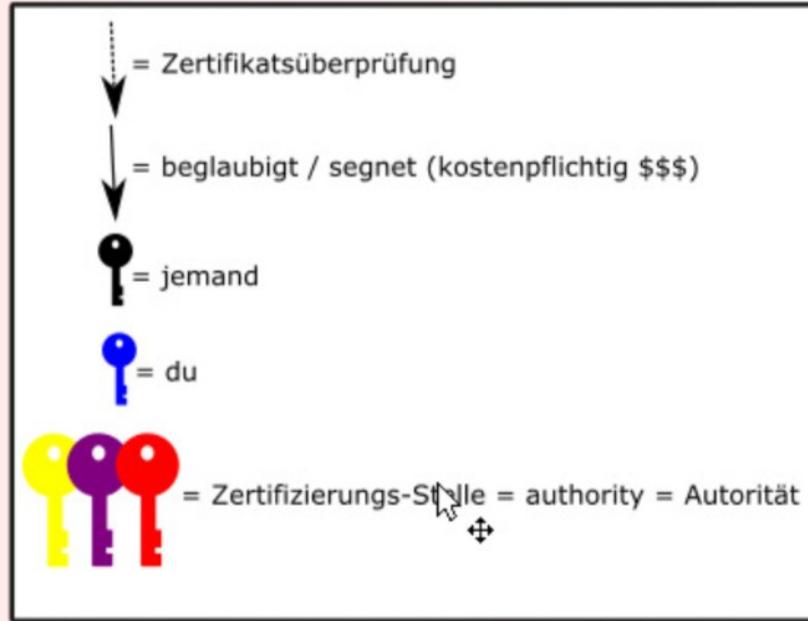


AUCTORITAS  
SIGNATORIA  
RADICALIS  
SANCTAE SEDIS



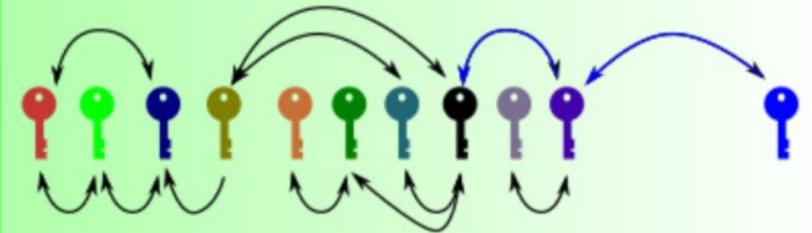
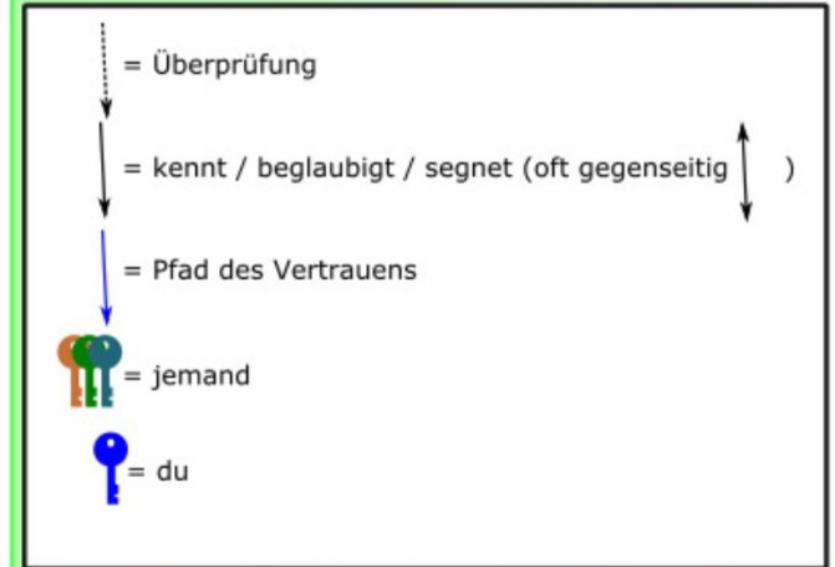
# Hierarchisches (CA-) Vertrauensmodell

~ LEGENDE ~



# Web-of-Trust- Vertrauensmodell

~ LEGENDE ~



# Anja muss auf ihren privaten Schlüssel aufpassen

- Jeder, der Anjas privaten Schlüssel besitzt, kann Anjas Emails lesen
- Jeder, der Anjas privaten Schlüssel besitzt, kann sich als Anja in Emails ausgeben
- Daher sollte Anja ihren privaten Schlüssel nur selbst erzeugen
- Mit einem langen Passwort gesichert auf dem Rechner abspeichern
- Oder nur auf separatem USB-Stick (Nitrokey, YubiKey, ...) erzeugen und sichern

# Welche Verfahren gibt es?

- S/MIME und PGP
- S/MIME
  - Basiert auf Zertifizierungsstellen
  - In Thunderbird, Outlook, iOS integriert, alternative Apps für Android
  - Nicht im Browser möglich
- PGP
  - Basiert auf Web of Trust oder direktem Schlüsselaustausch
  - Addons für Thunderbird, Outlook; alternative Apps für iOS und Android
  - Als Browser-Addon Mailvelope für Webmail von GMX, Web.de und Gmail verfügbar

# S/MIME

- Was braucht Anja?
- Wie richtet sie es ein?
- Was braucht Bernd?
- Wie kommunizieren Anja und Bernd sicher (signiert und verschlüsselt?)

# Was braucht Anja: Ein Zertifikat

The image shows a browser window with two tabs. The left tab is the SwissSign website, and the right tab is the Actalis Service Portal.

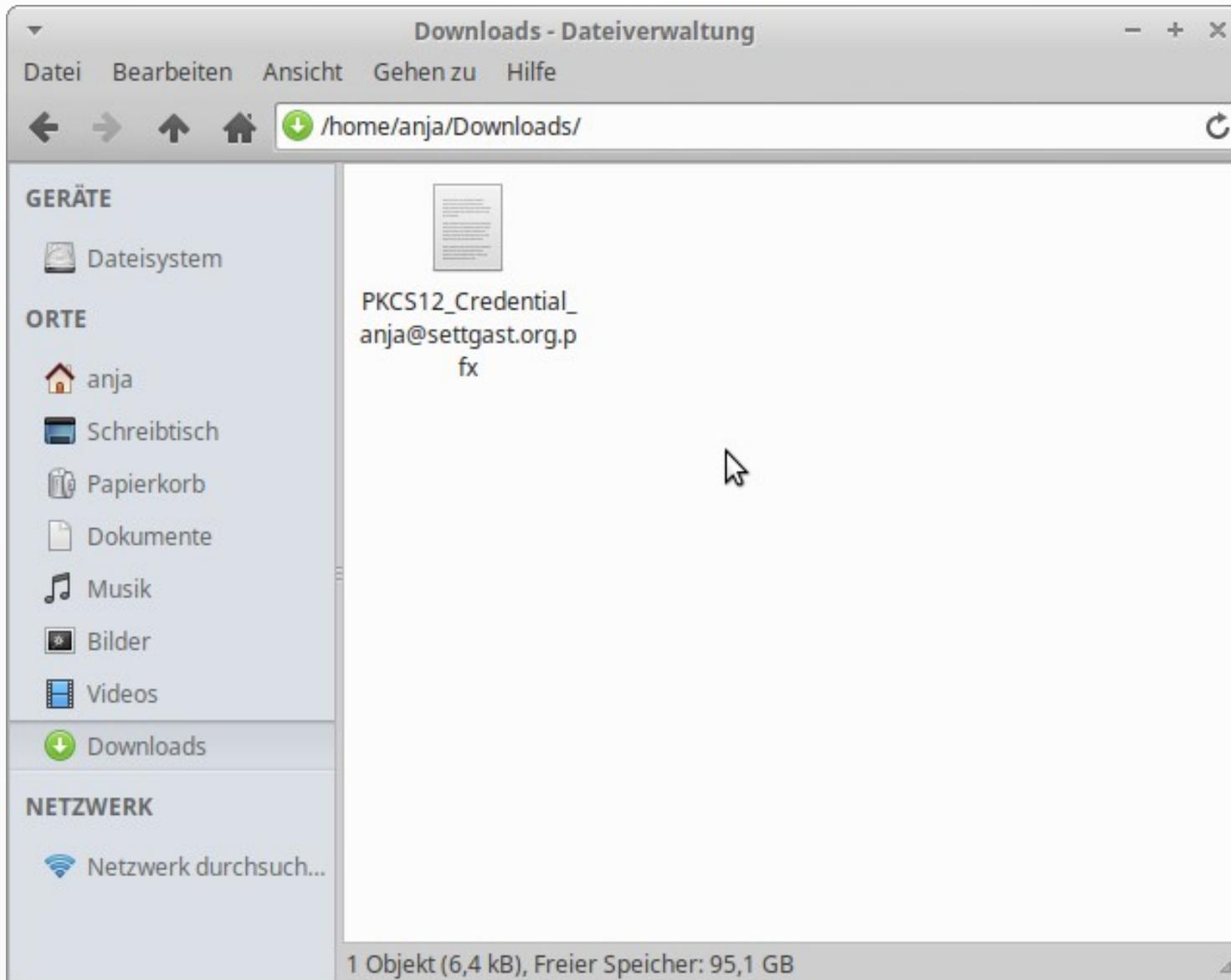
**SwissSign Website:**

- URL: <https://www.swissign.com>
- Navigation: SSL, E-Mail, Signing, Manager
- Dropdown menu: E-Mail ID Gold, E-Mail ID Silver
- Text: **Finden Sie Zertifikat**
- Button: **Zum Shop**
- Footer: SwissSign AG verwendet Cookies, um Ihr Online-Erlebnis auf [swissign.com](https://www.swissign.com) akzeptieren Sie unsere Cookie Policy. <https://www.swissign.com/email/email-id-silver.html>

**Actalis Service Portal:**

- URL: <https://extrassl.actalis.it/portal/uapub/doSendEmail>
- Logos: ACTALIS, ARUBA GROUP
- Section: **Free Email Certificate**
- Message: **Free Email Certificate** (with envelope icon)
- Success message: **We sent you a e-mail, please check your e-mail and enter the code that we sent you in the Verification code field** (with green checkmark icon)
- Step 1 - Validity check of the Email:
  - Email:
  - Button: SEND VERIFICATION EMAIL
  - Verification code:
  - Captcha:
  - Captcha image:
  - Button: Regenerate
- Step 2 - Request Certificate:
  - Link: [Free S/MIME Certificates Terms & Conditions](#)
  - Checkbox:  I declare to have read and accept the above terms and conditions
  - Link: [Approval of specific clauses related to Free S/MIME Certificates](#)

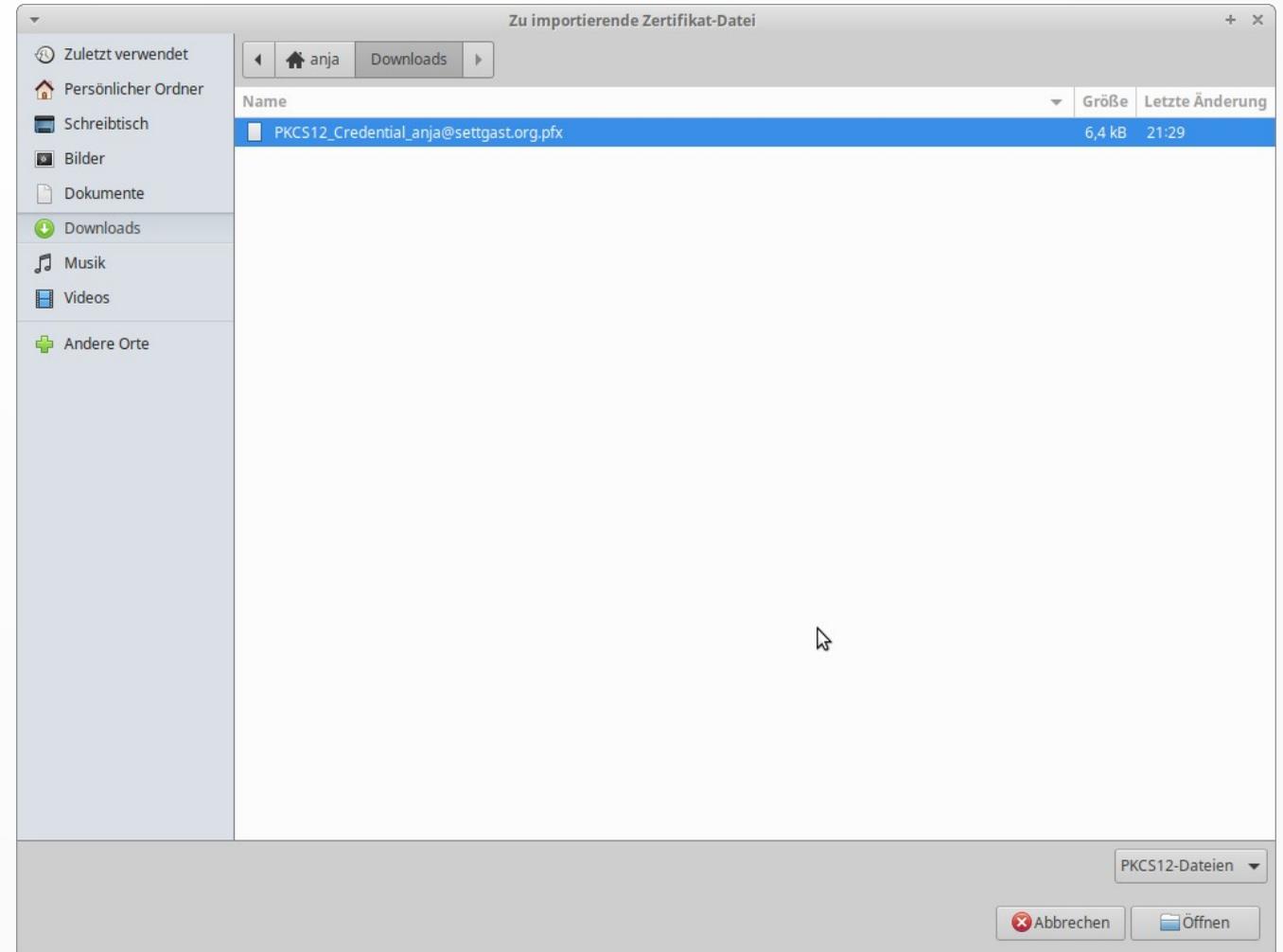
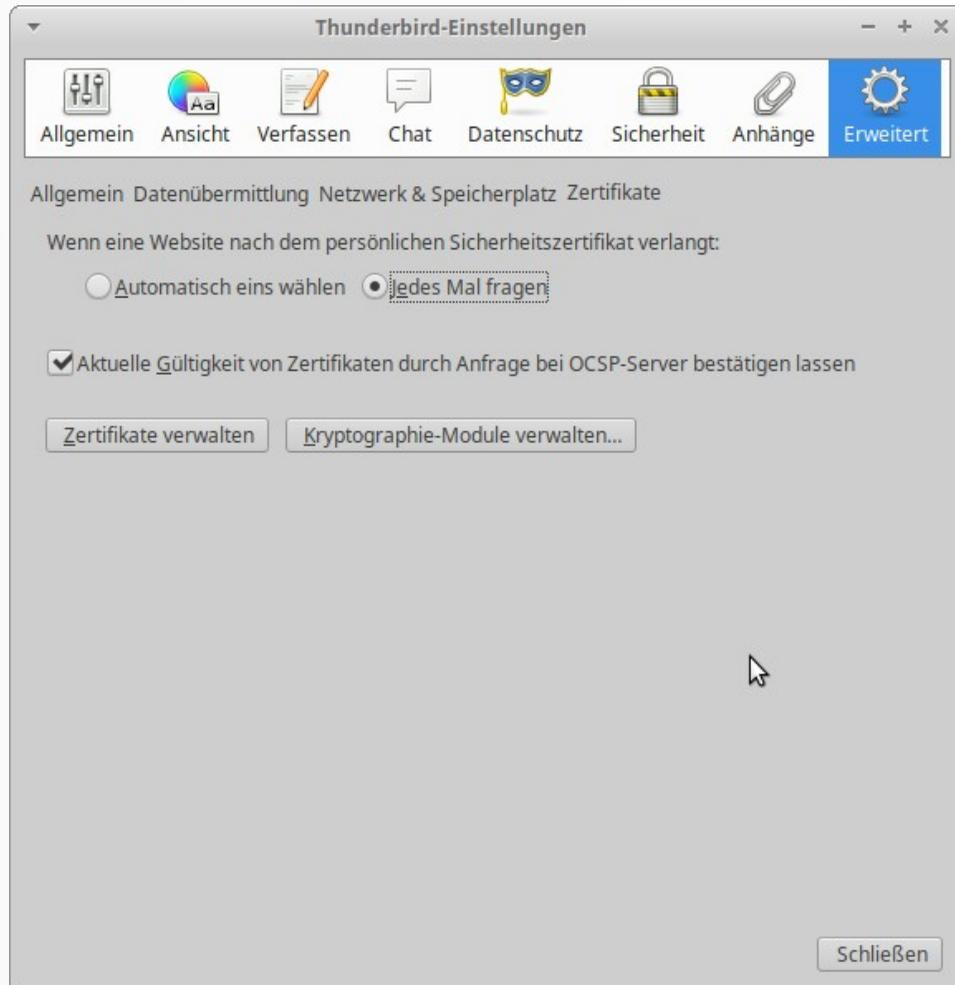
# Ergebnis: Zertifikatsdatei



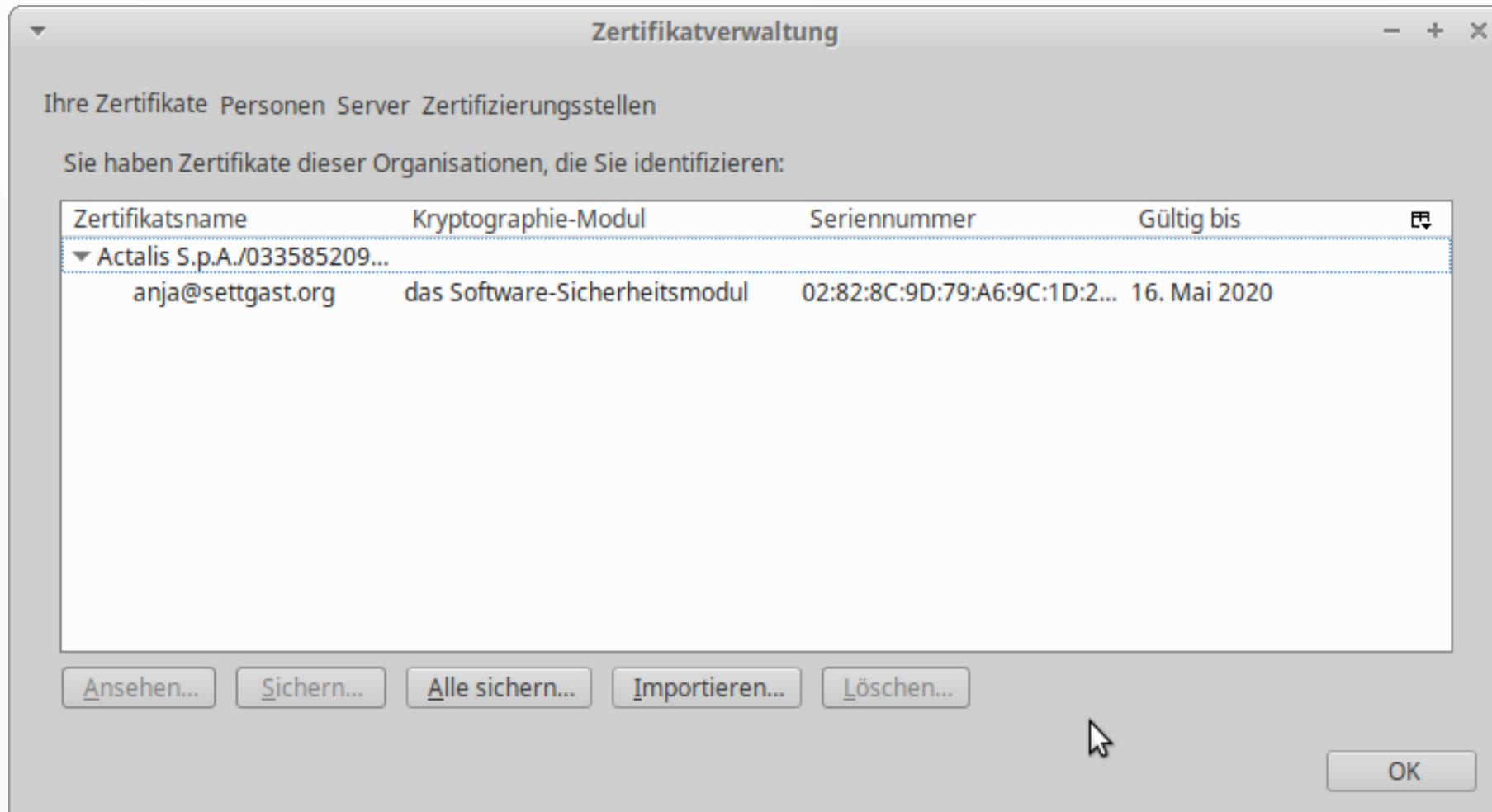
# Was muss Anja einrichten?

- Zertifikat in Thunderbird importieren und im Account konfigurieren

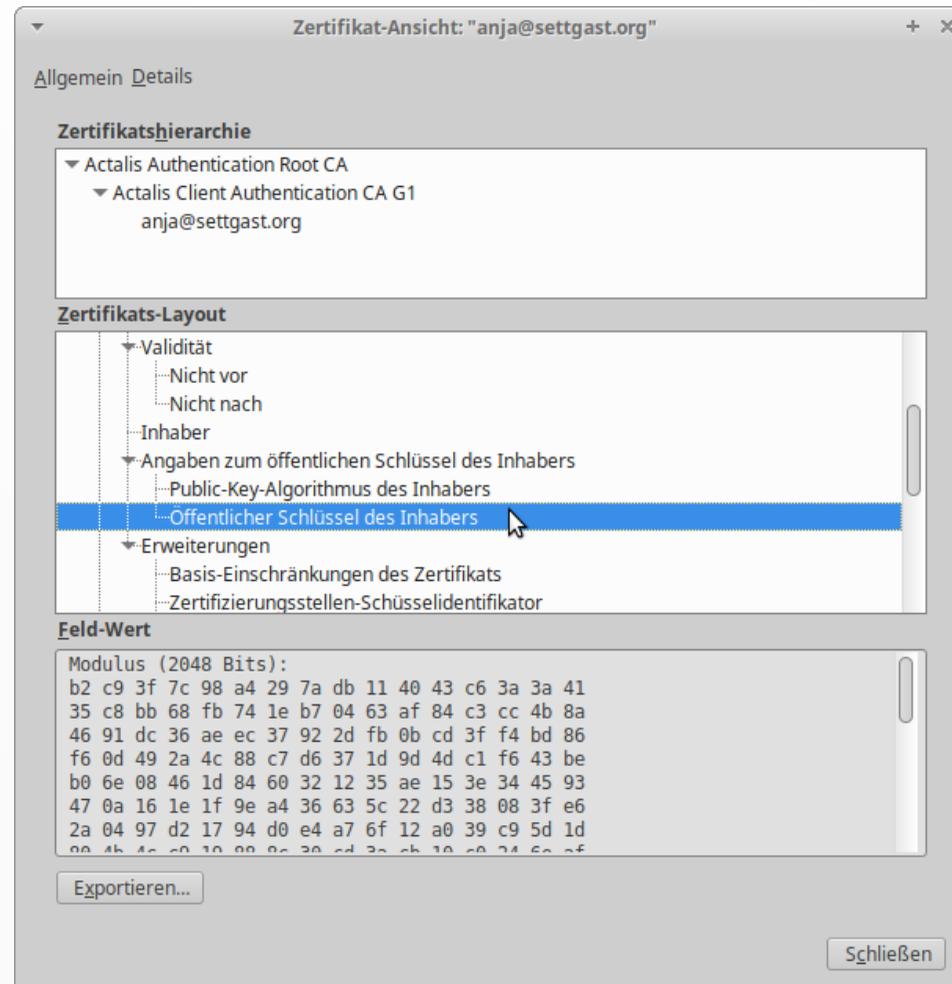
# Zertifikate verwalten



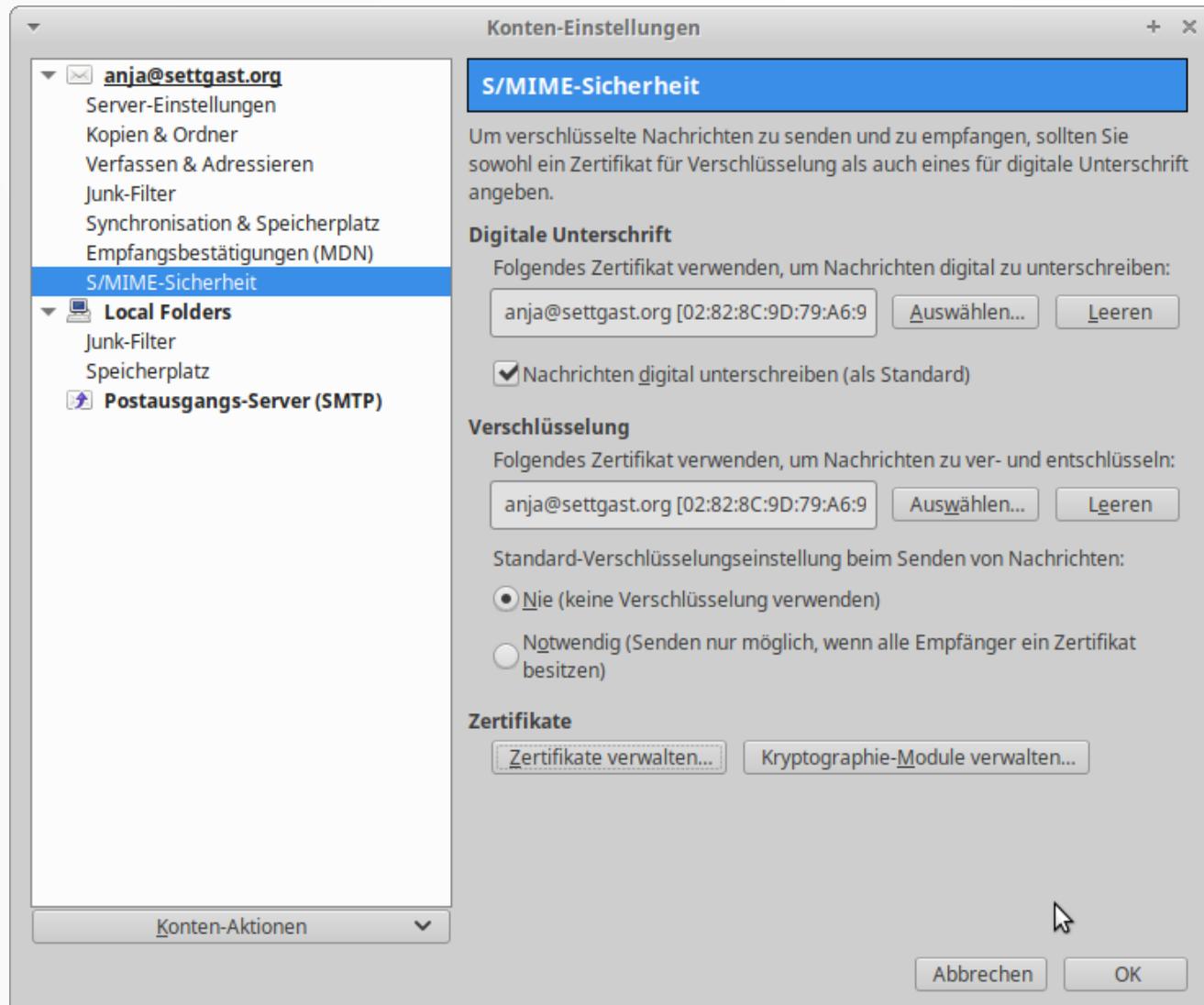
# Zertifikat importiert



# Was steckt im Zertifikat?



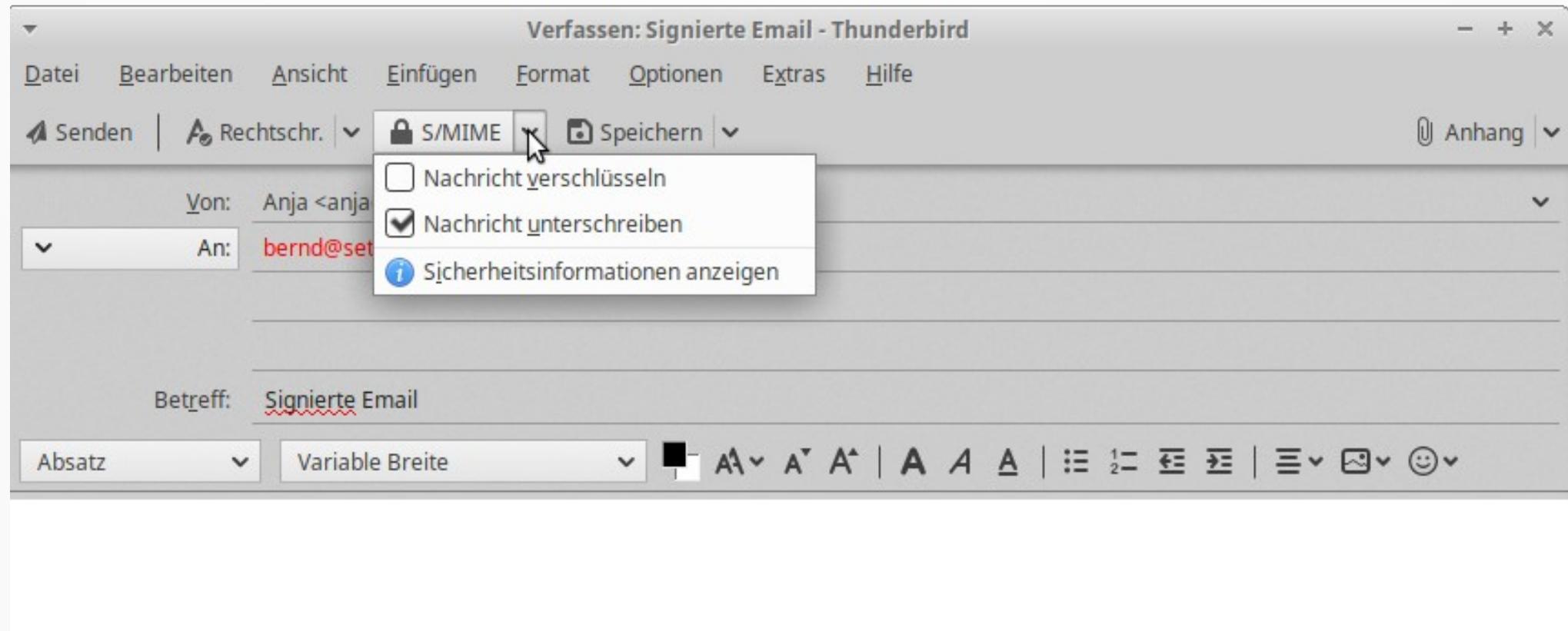
# Email-Konto konfigurieren



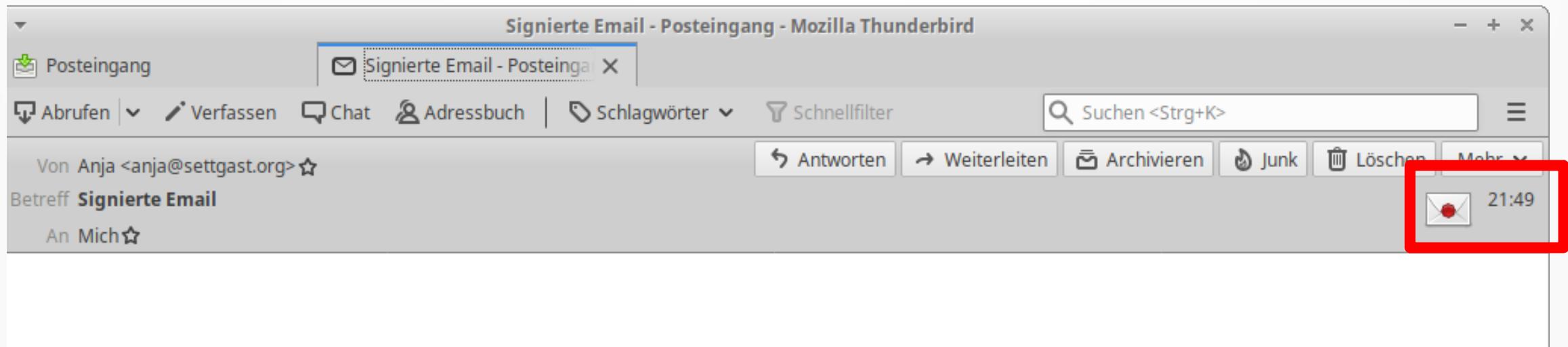
- Zertifikat zum Signieren auswählen
- „Nachrichten digital unterschreiben (als Standard)“ auswählen
- Zertifikat für Verschlüsselung auswählen

# Was braucht Bernd?

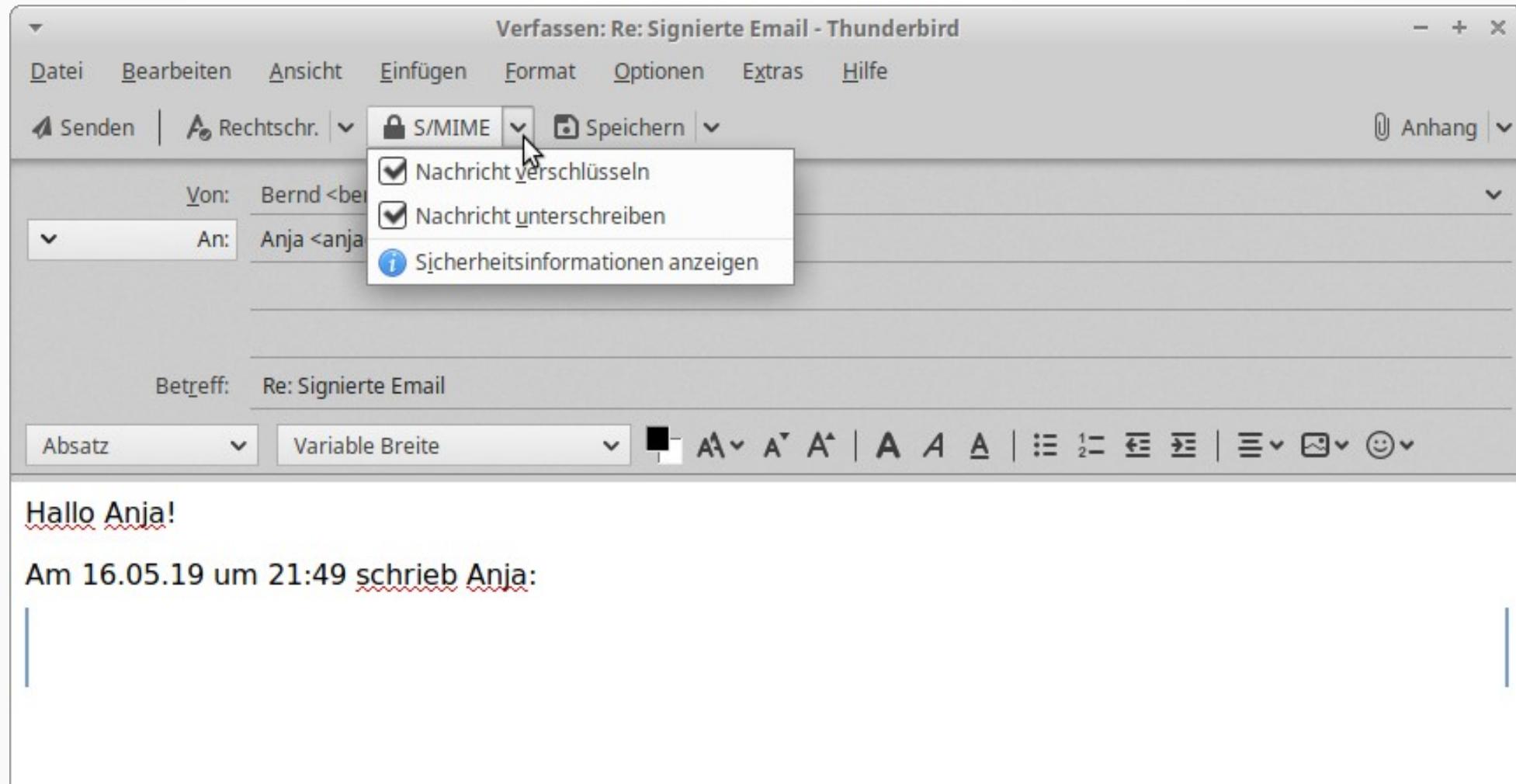
- Öffentlichen Schlüssel von Anja, im Zertifikat enthalten
- Anja schickt signierte Email an Bernd



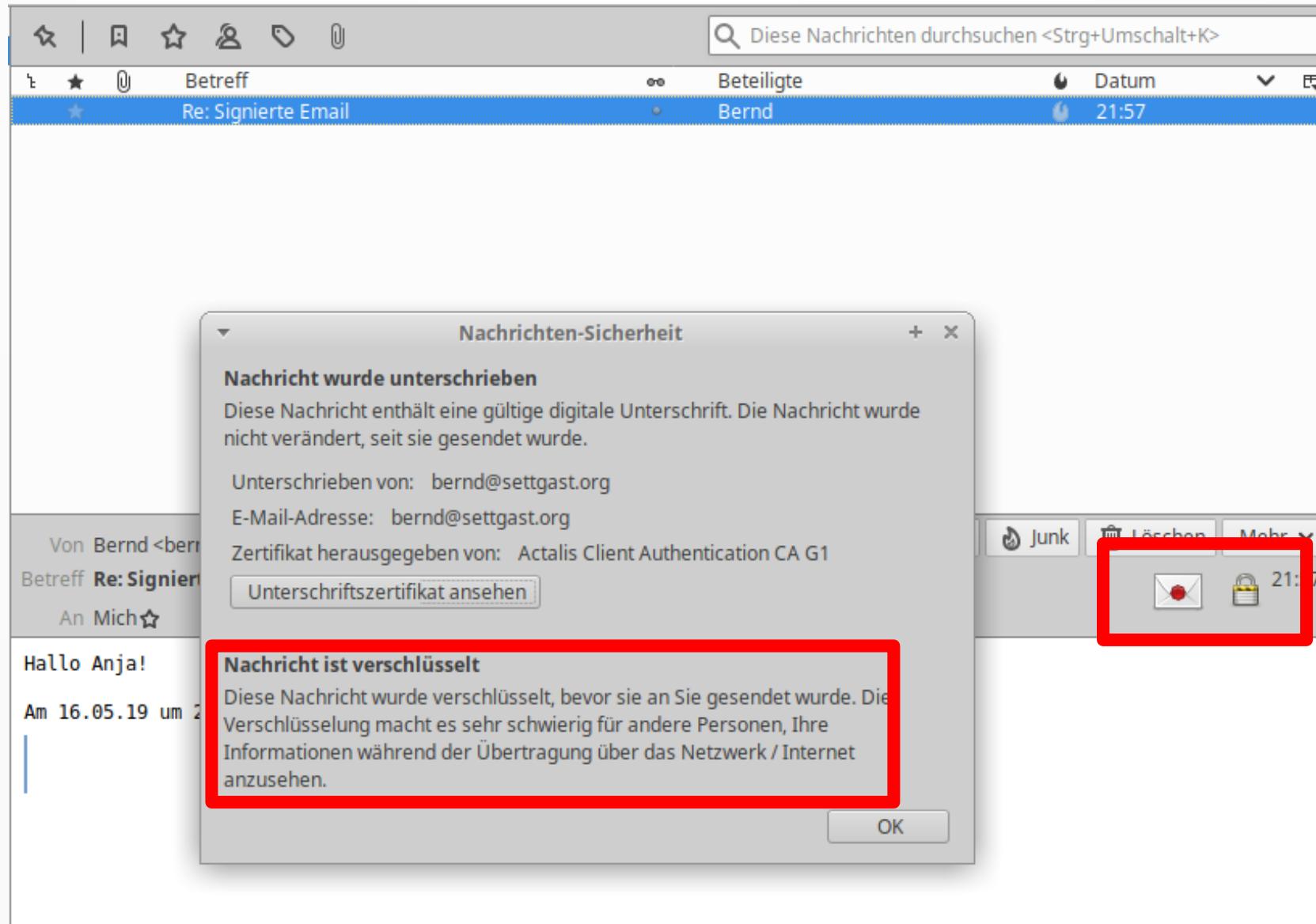
# So sieht das bei Bernd aus



# Bernd schickt signierte und verschlüsselte Email an Anja



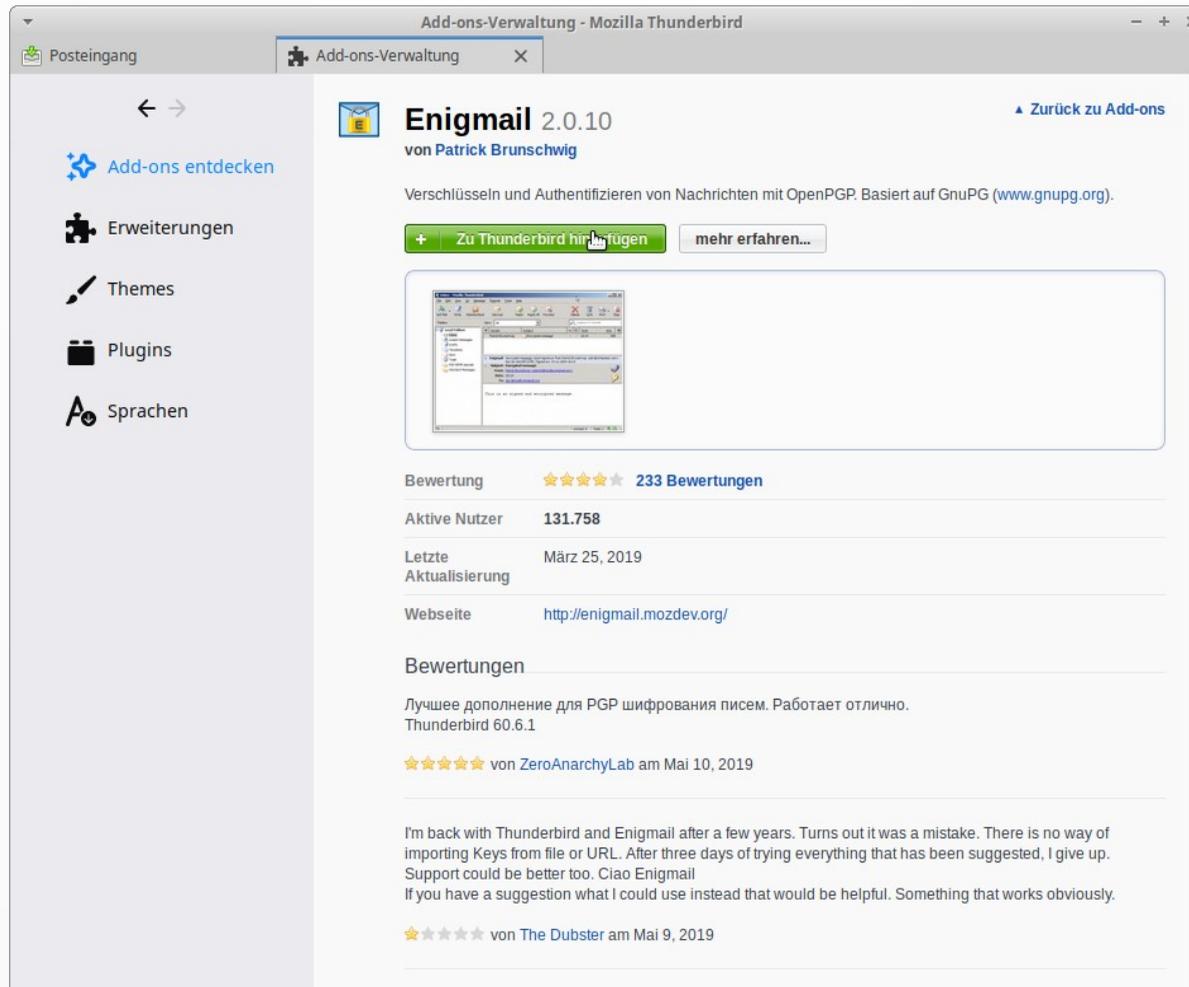
# So sieht das bei Anja aus



# PGP

- Was braucht Anja?
- Wie richtet sie es ein?
- Was braucht Bernd?
- Wie kommunizieren Anja und Bernd sicher (signiert und verschlüsselt?)

# Was braucht Anja?



The screenshot shows the Mozilla Thunderbird Add-ons Manager window. The main content area displays the details for the 'Enigmail 2.0.10' add-on by Patrick Brunschwig. The add-on is described as a tool for encrypting and authenticating messages using OpenPGP. It features a green 'Zu Thunderbird hinzufügen' button and a 'mehr erfahren...' link. Below the description, there is a small screenshot of the add-on's interface. The page also shows the add-on's rating (5 stars, 233 reviews), the number of active users (131,758), the last update date (March 25, 2019), and the website (http://enigmail.mozdev.org/). There are two user reviews visible, both with 5-star ratings.

Posteingang Add-ons-Verwaltung

← →

Add-ons entdecken

Erweiterungen

Themes

Plugins

Sprachen

**Enigmail 2.0.10** Zurück zu Add-ons  
von Patrick Brunschwig

Verschlüsseln und Authentifizieren von Nachrichten mit OpenPGP. Basiert auf GnuPG ([www.gnupg.org](http://www.gnupg.org)).

+ Zu Thunderbird hinzufügen mehr erfahren...



Bewertung ★★★★★ 233 Bewertungen

Aktive Nutzer 131.758

Letzte Aktualisierung März 25, 2019

Webseite <http://enigmail.mozdev.org/>

Bewertungen

Лучшее дополнение для PGP шифрования писем. Работает отлично.  
Thunderbird 60.6.1

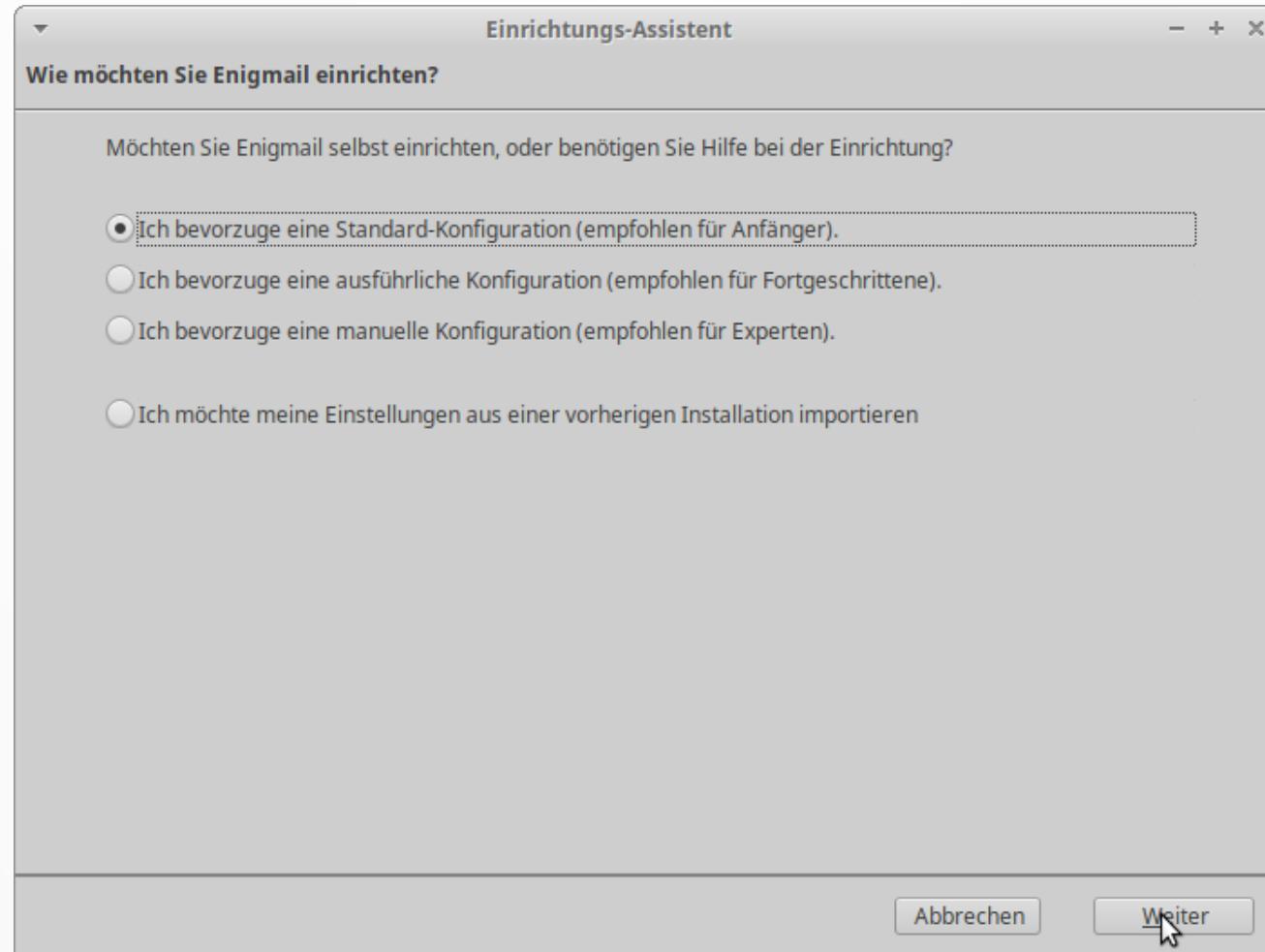
★★★★★ von ZeroAnarchyLab am Mai 10, 2019

I'm back with Thunderbird and Enigmail after a few years. Turns out it was a mistake. There is no way of importing Keys from file or URL. After three days of trying everything that has been suggested, I give up. Support could be better too. Ciao Enigmail

If you have a suggestion what I could use instead that would be helpful. Something that works obviously.

★★★★★ von The Dubster am Mai 9, 2019

# Wie richtet sie es ein?



# Schlüsselpaar erzeugen

Einrichtungs-Assistent

**OpenPGP-Schlüssel erzeugen**  
Neues Schlüsselpaar erstellen

Dieser Dialog wird ein Paar von zwei Schlüsseln erzeugen:  
Mit Ihrem **öffentlichen Schlüssel** können **Andere** E-Mails an Sie verschlüsseln (und von Ihnen signierte Nachrichten überprüfen). Sie dürfen ihn jedem geben.  
Ihr **privater Schlüssel** ist **nur für Sie**, um damit Mails an Sie zu entschlüsseln und um Mails, die Sie schicken, zu signieren. Sie sollten ihm niemandem geben.

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:  
Anja <anja@settgast.org> - anja@settgast.org

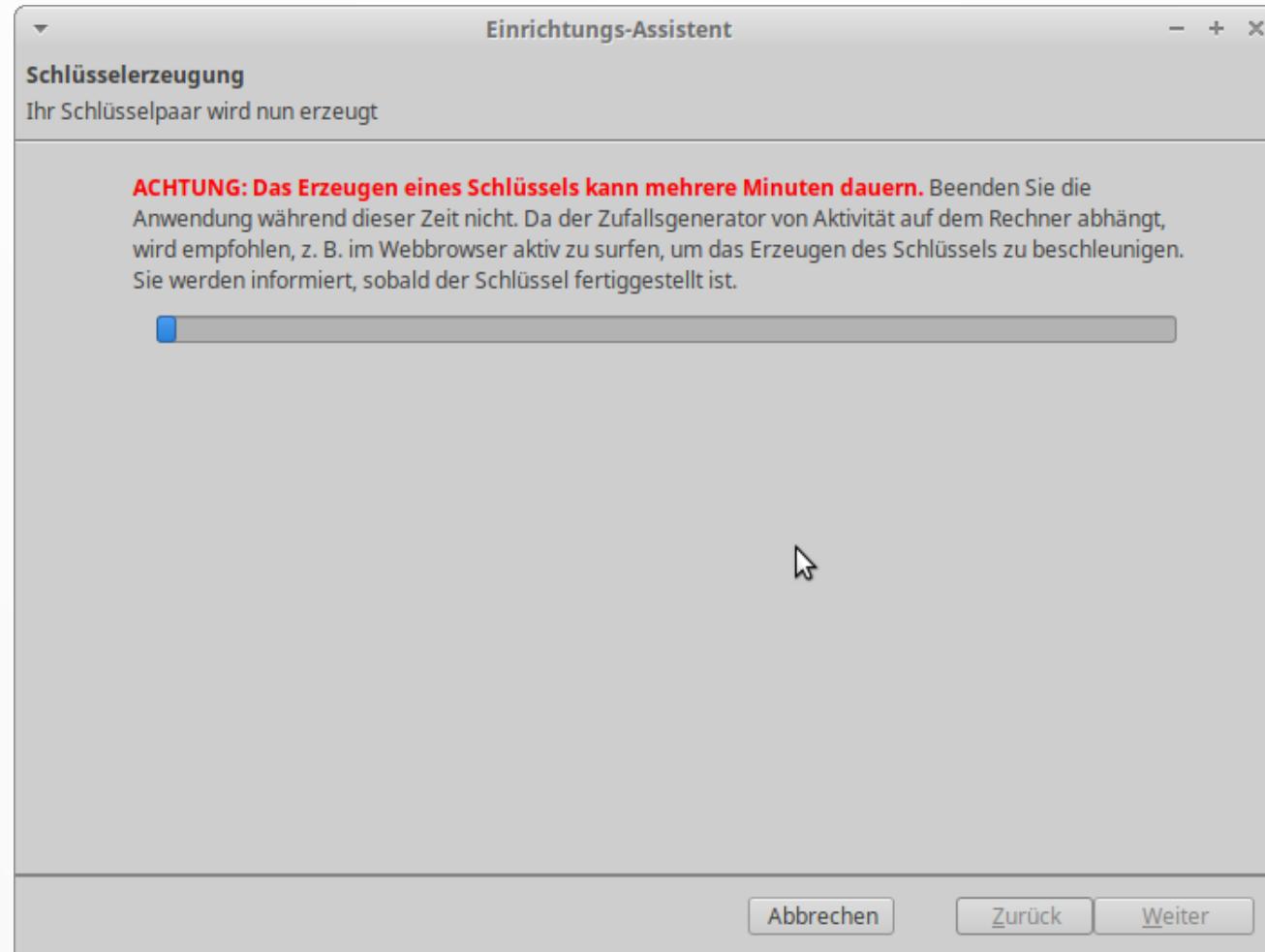
Passphrase

Bitte bestätigen Sie Ihre Passphrase durch erneutes Eingeben

Qualität der Passphrase:

Abbrechen Zurück Weiter

# Schlüsselpaar erzeugen

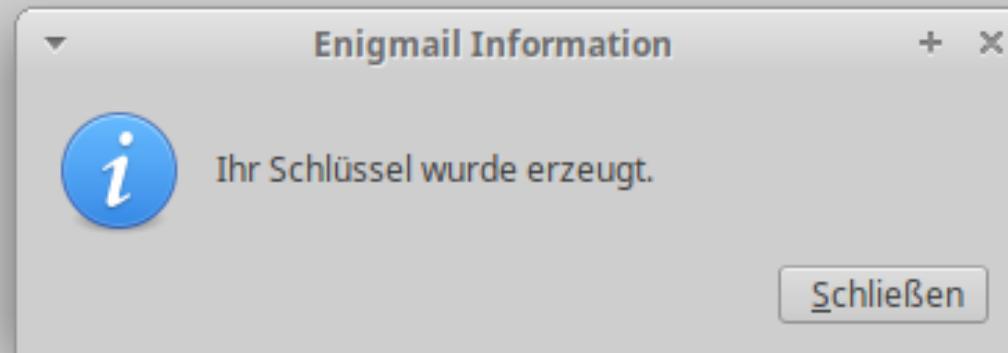


# Schlüsselpaar erzeugt

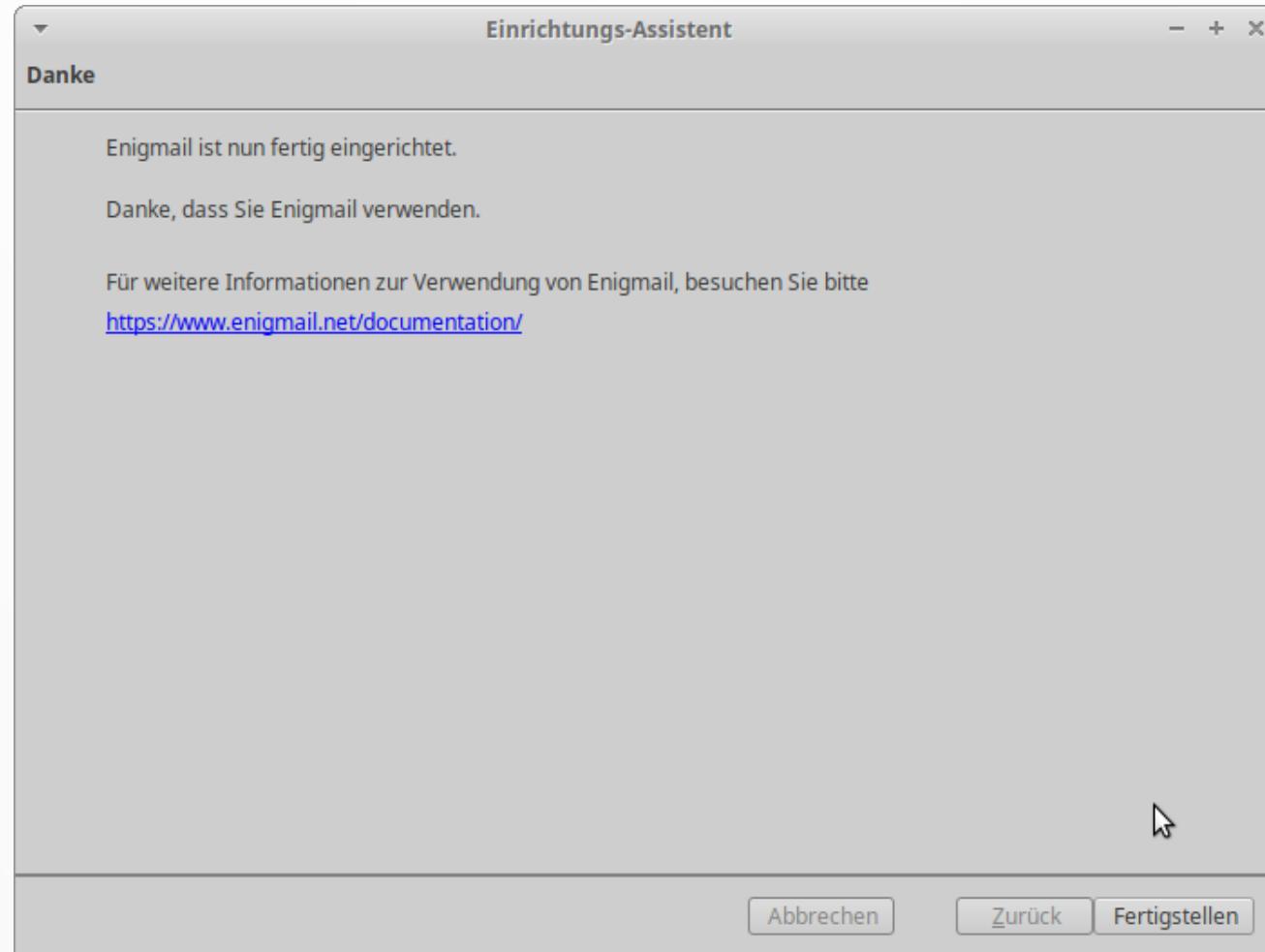
## Schlüsselerzeugung

Ihr Schlüsselpaar wird nun erzeugt

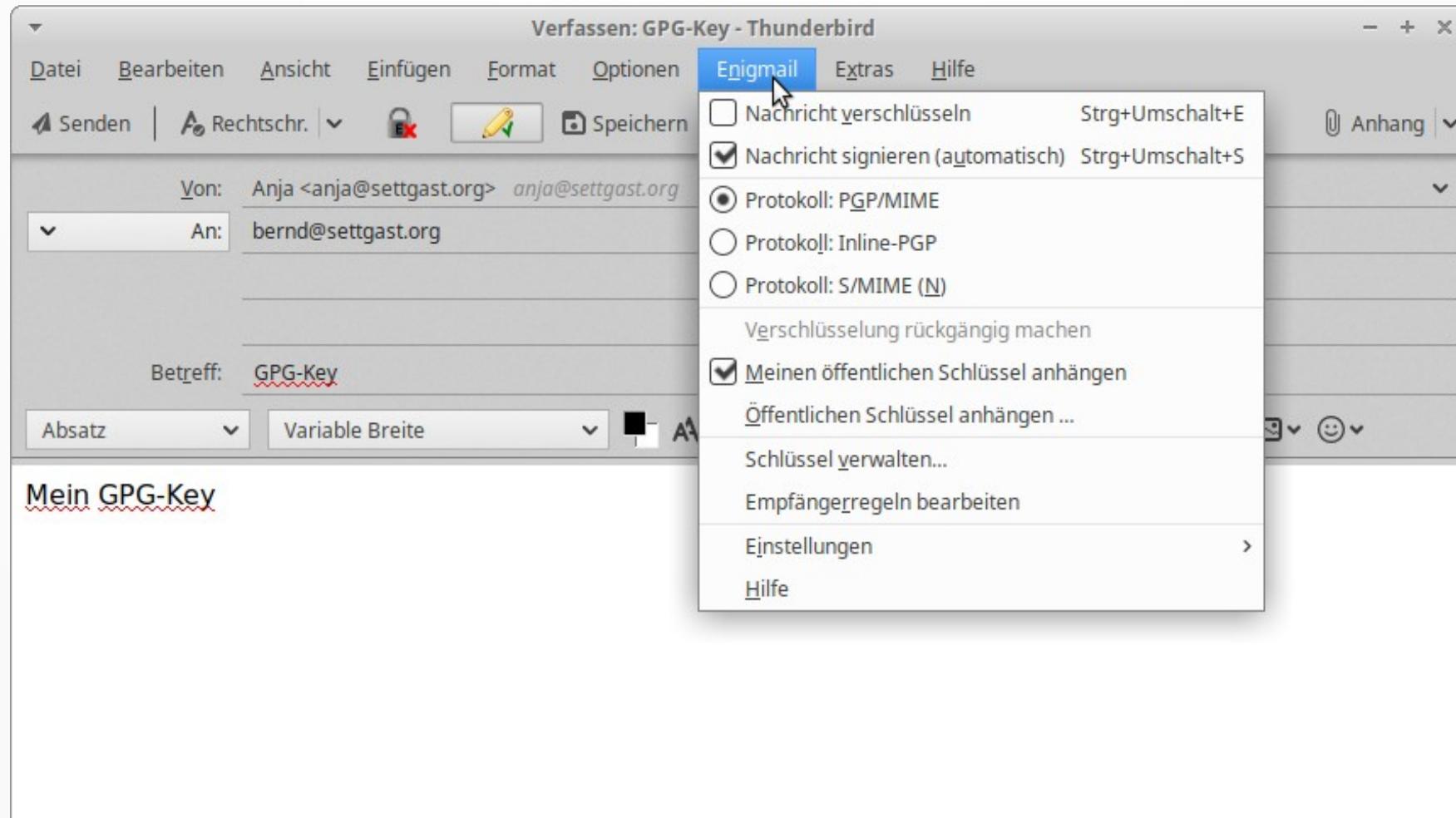
**ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern.** Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen, z. B. im Webbrowser aktiv zu surfen, um das Erzeugen des Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.



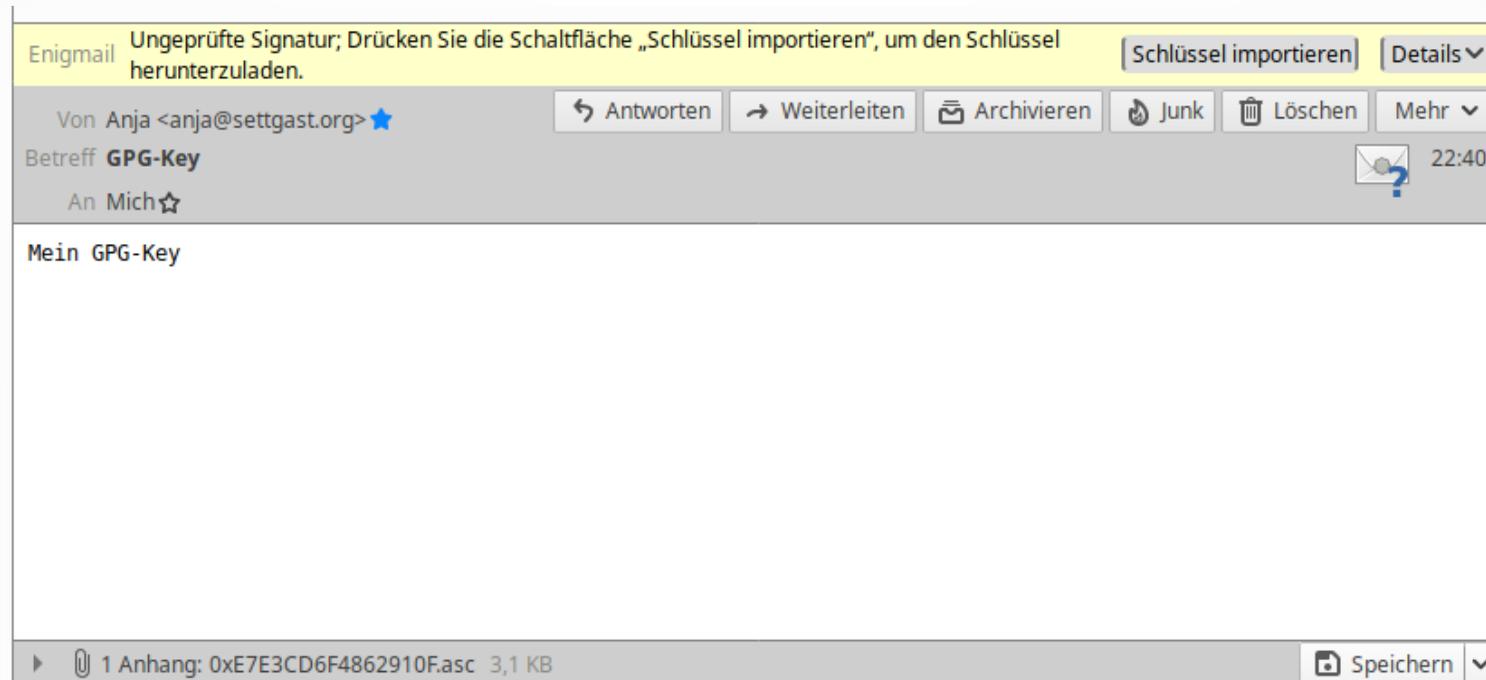
# Einrichtung abgeschlossen



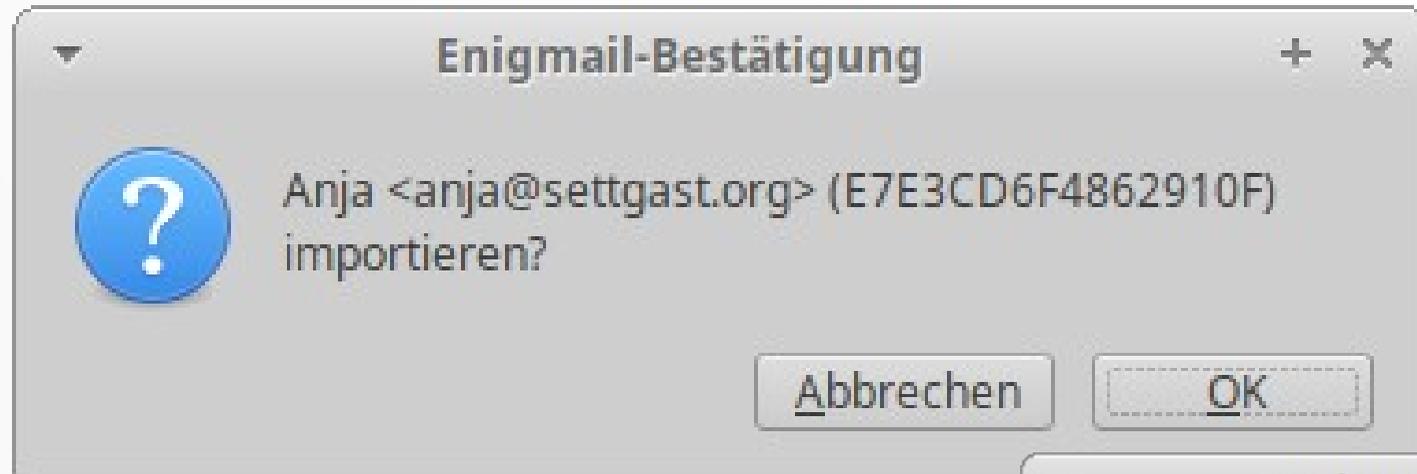
# Anja schickt GPG-Key an Bernd



# So sieht das bei Bernd aus



# Bernd prüft Schlüssel von Anja



# Bernd prüft Schlüssel von Anja

**Enigmail - Schlüssel signieren** + ×

Zu signierender Schlüssel: Anja <anja@settgast.org> - 0xE7E3CD6F4862910F  
Fingerabdruck: 5052 3B5F EAD6 E936 6A29 A3CB E7E3 CD6F 4862 910F

Schlüssel zum Signieren: Bernd <bernd@settgast.org> - 0x0A61498AA8222ABC ▼

Hinweis: Sie müssen das Besitzervertrauen Ihrer eigenen Schlüssel auf „Absolut“ setzen, damit sie hier angezeigt werden.

**Wie sorgfältig haben Sie überprüft, ob dieser Schlüssel tatsächlich dem oben genannten Inhaber(n) gehört?**

Keine Antwort

Ich habe es überhaupt nicht überprüft

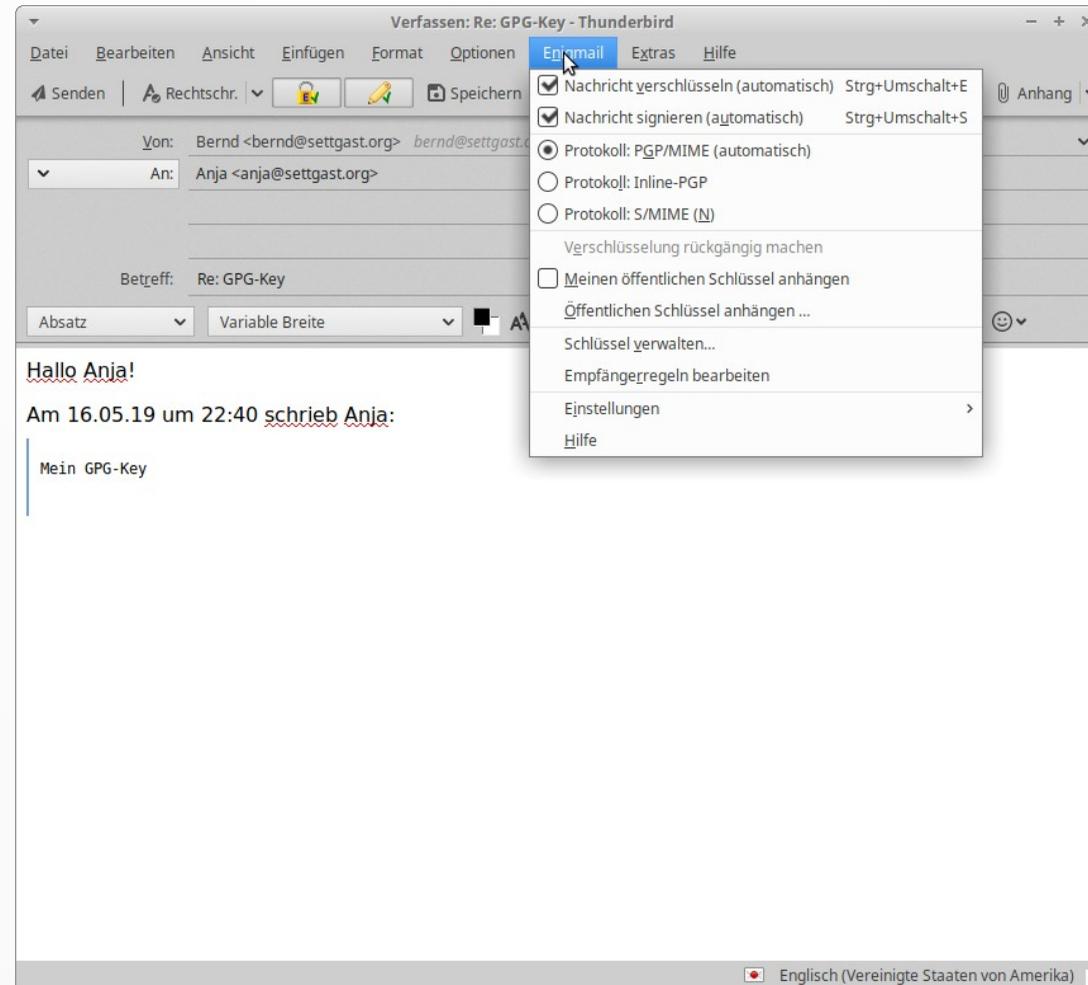
Ich habe es nur einfach überprüft

Ich habe es sehr genau überprüft

Lokal signieren (kann nicht exportiert werden)

Abbrechen OK

# Bernd schickt signierte und verschlüsselte Email



# So sieht das bei Anja aus

Enigmail Entschlüsselte Nachricht; Ungeprüfte Signatur; Drücken Sie die Schaltfläche „Schlüssel importieren“, um den Schlüssel herunterzuladen. Schlüssel importieren Details

Antworten Weiterleiten Archivieren Junk Löschen Mehr

Von Bernd <bernd@settgast.org> ★

Betreff **Re: GPG-Key** 22:48

An Mich ☆

Hallo Anja!

Am 16.05.19 um 22:40 schrieb Anja:

Mein GPG-Key

**Enigmail Information**

Enigmail-Sicherheitsinfo:

Entschlüsselte Nachricht  
Ungeprüfte Signatur  
Öffentlicher Schlüssel 0A61498AA8222ABC wird zur Überprüfung der Signatur benötigt

Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:  
0x39B00240E0A2430A (Anja <anja@settgast.org>),  
0x20AFA11B4BF848D3

Schließen

# Web of Trust: Bernd vertraut Anja, dass sie andere Schlüssel sorgfältig prüft

Enigmail - Besitzervertrauen festlegen

Vertrauenswürdiger Schlüssel: Anja <anja@settgast.org> - 0xE7E3CD6F4862910F

Wie weit trauen Sie dem Besitzer des Schlüssels zu, die anderen Schlüssel ordnungsgemäß zu signieren?

Unbekannt (Noch nicht zugewiesen)

Nicht vertrauenswürdig (Nicht vertrauenswürdig, um Schlüssel ordnungsgemäß zu signieren)

Gering (Etwas vertrauenswürdig, um Schlüssel ordnungsgemäß zu signieren)

**Komplett (Voll vertrauenswürdig, um Schlüssel ordnungsgemäß zu signieren)**

Absolutes Vertrauen (Nur für Schlüssel, die man selbst besitzt)

Abbrechen OK

# Was haben wir gesehen?

- Motivation
- Wie funktioniert Verschlüsselung?
- Wie funktioniert Email-Verschlüsselung?
- Welche Verfahren gibt es?
- S/MIME – Wie geht es konkret?
- PGP – Wie geht es konkret?

**Vielen Dank für Ihre Aufmerksamkeit**