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
  - Verschlüsselungverfahren

Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

Bernd

Asymmetrische Verschlüsselung

Bernd

Anja

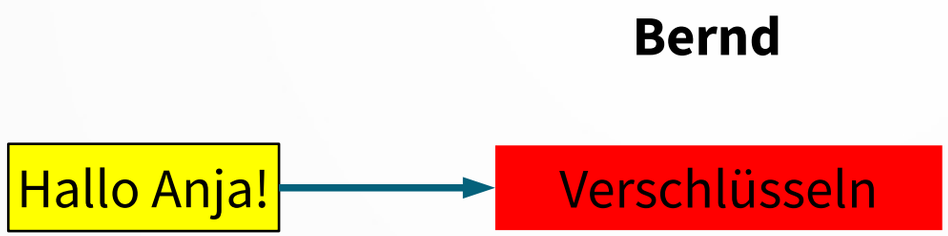
Asymmetrische Verschlüsselung

Bernd

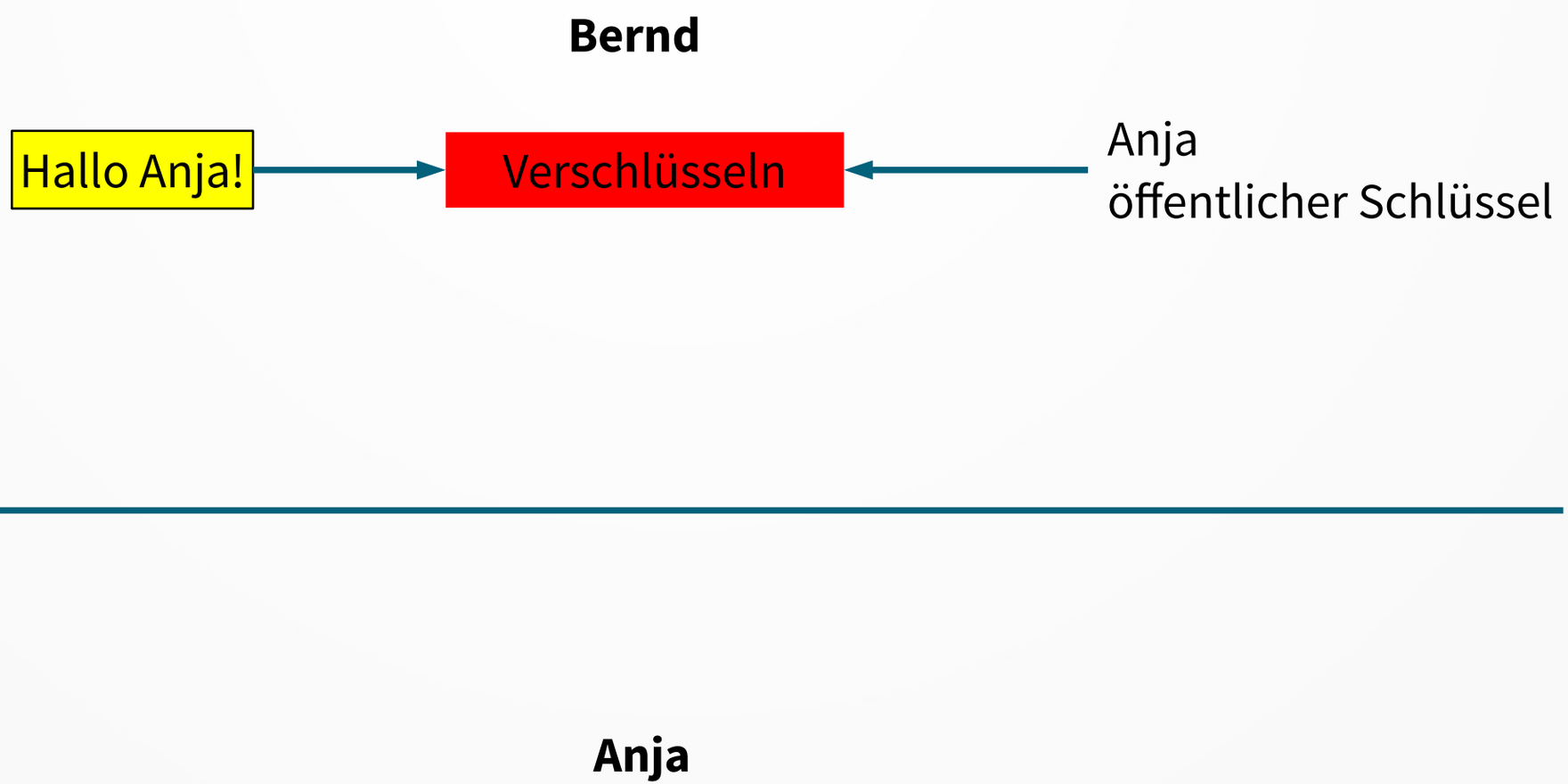
Hallo Anja!

Anja

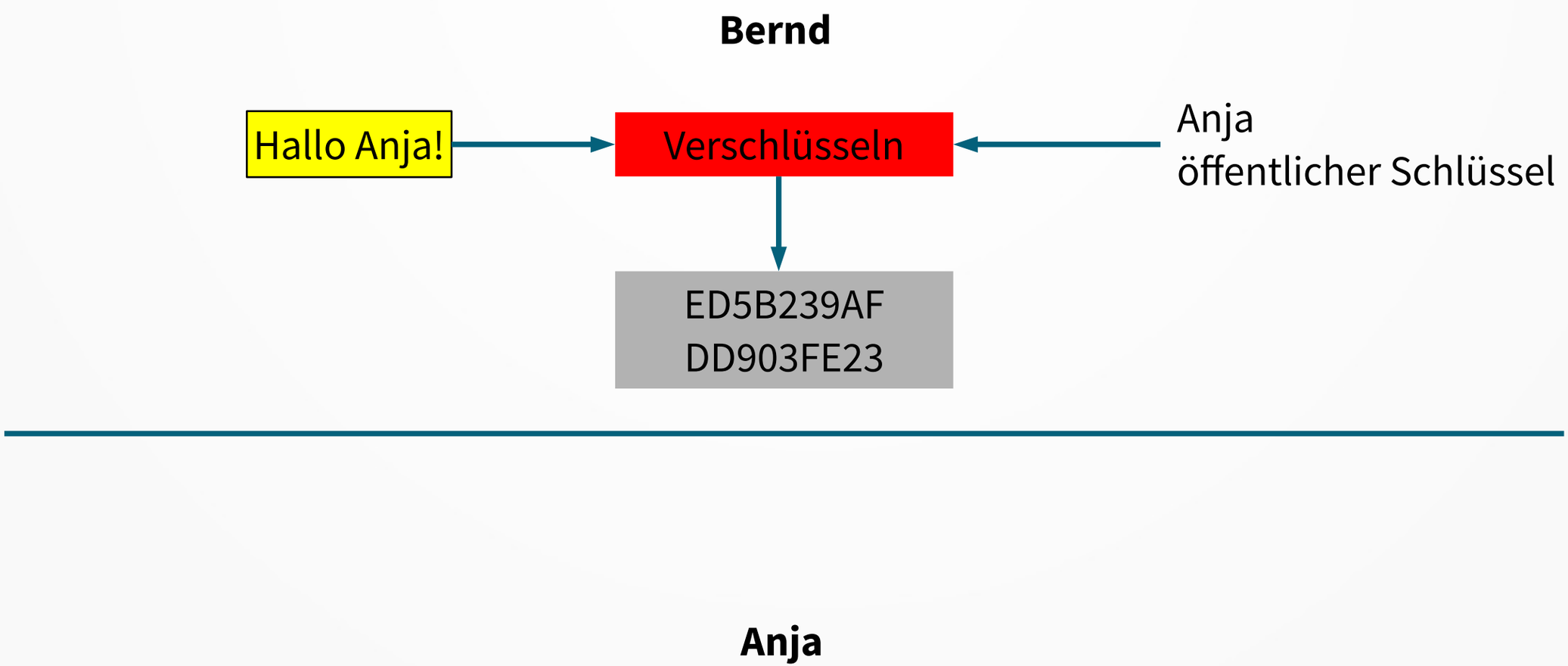
Asymmetrische Verschlüsselung



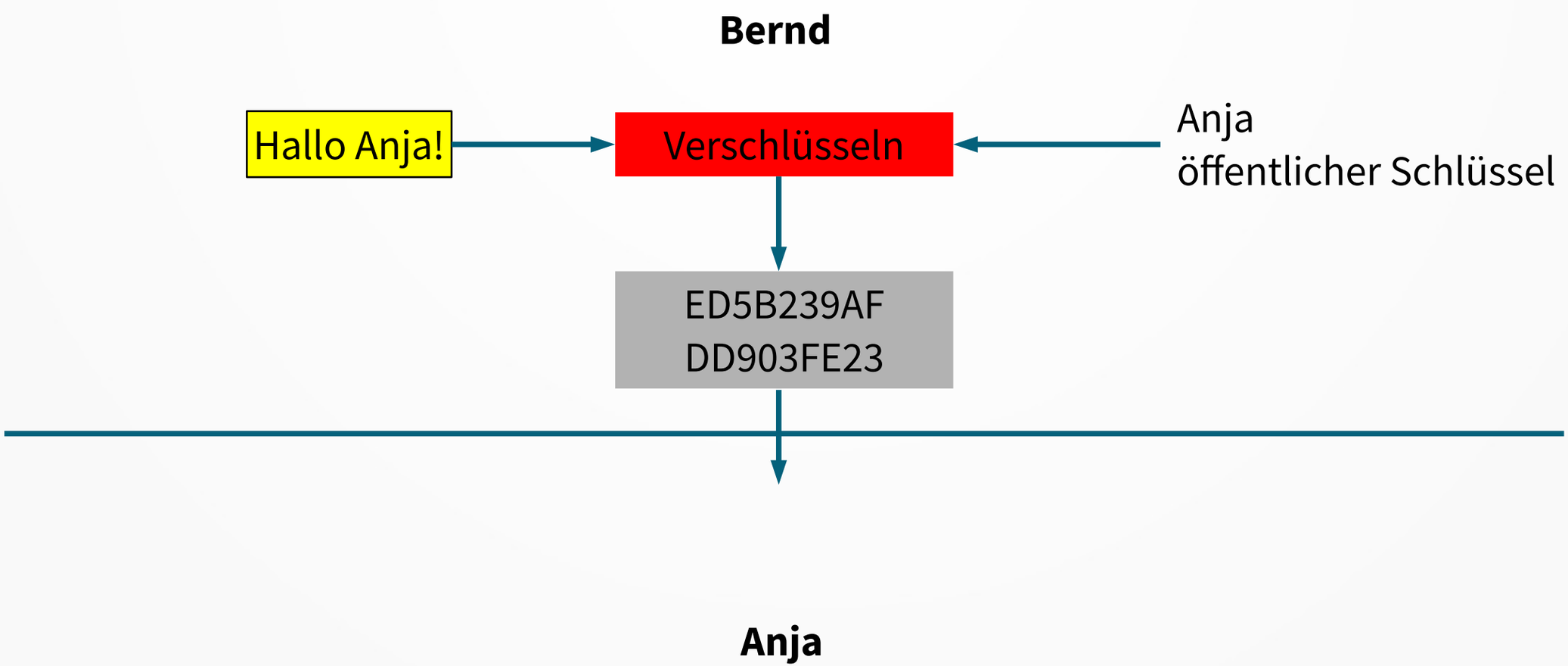
Asymmetrische Verschlüsselung



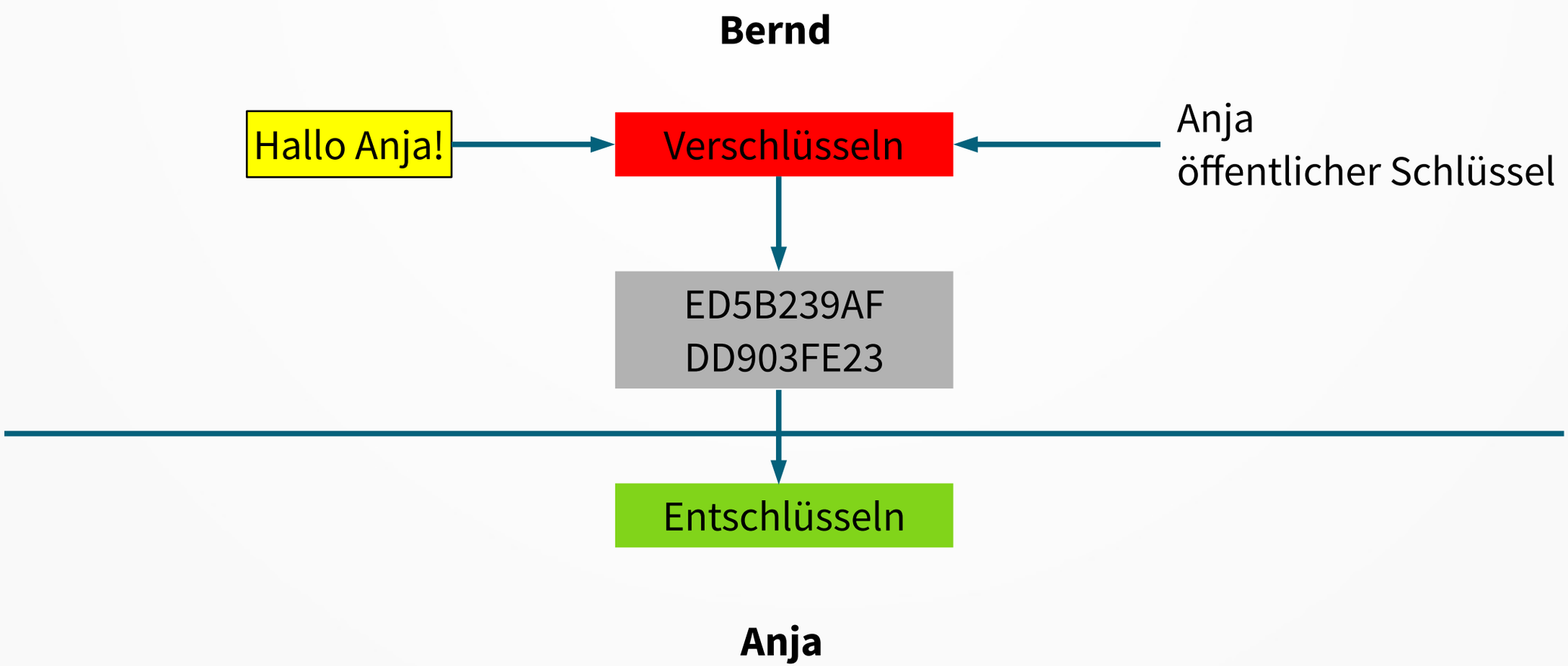
Asymmetrische Verschlüsselung



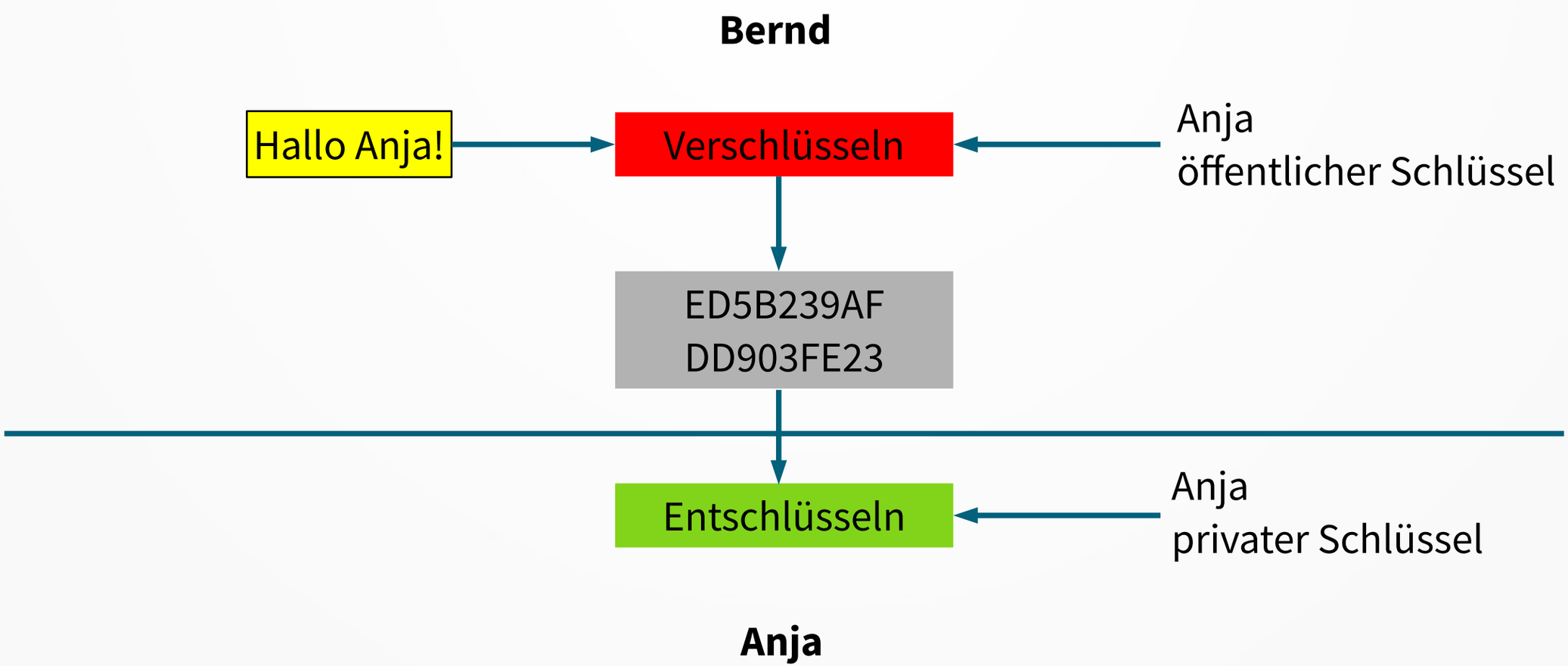
Asymmetrische Verschlüsselung



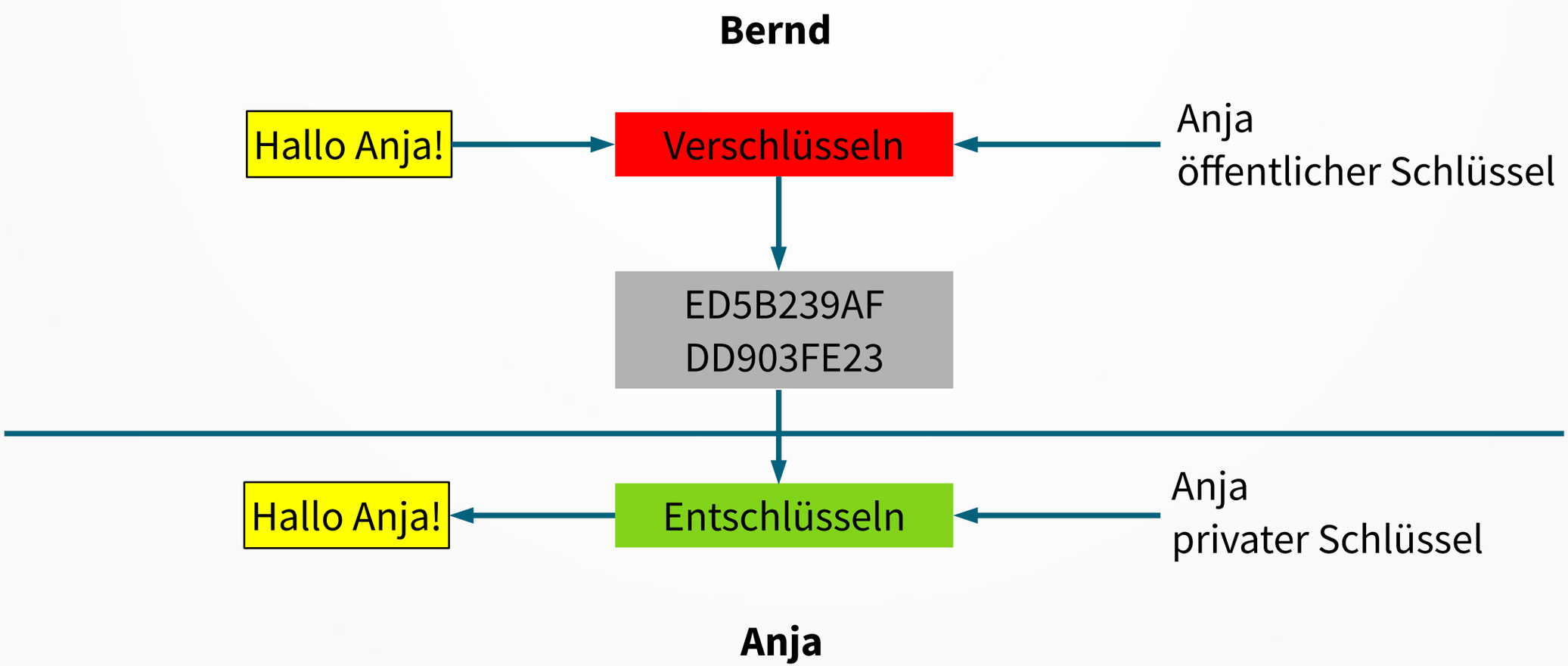
Asymmetrische Verschlüsselung



Asymmetrische Verschlüsselung



Asymmetrische Verschlüsselung



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

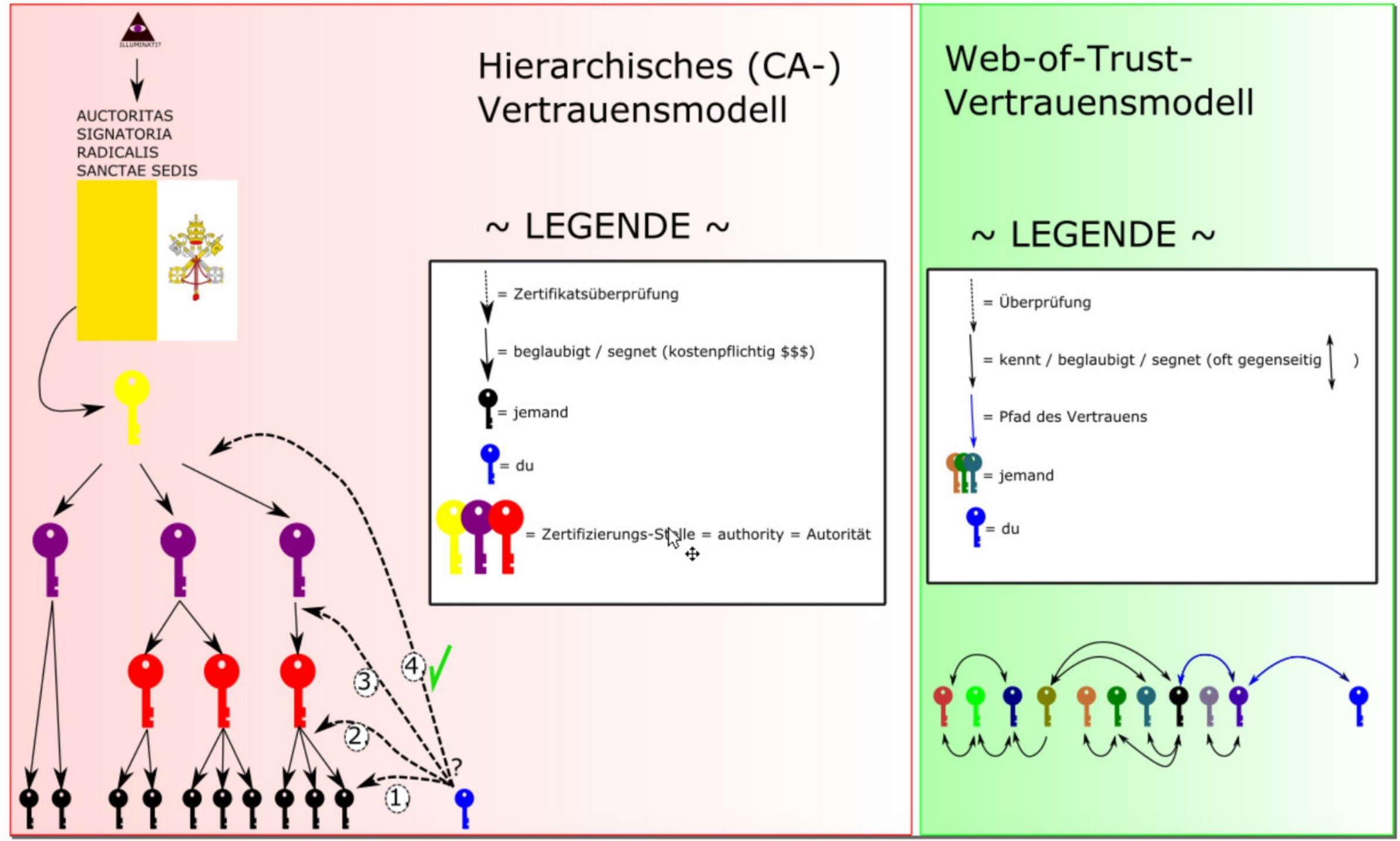
- Bernd schickt Anja eine Email mit dem öffentlichen Schlüssel
- Bernd lädt seinen öffentlichen Schlüssel auf sog. Keyserver hoch und Anja lädt ihn von dort herunter
- Öffentlicher Schlüssel darf/muss verteilt werden (wie der Name „öffentlich“ schon sagt)

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



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

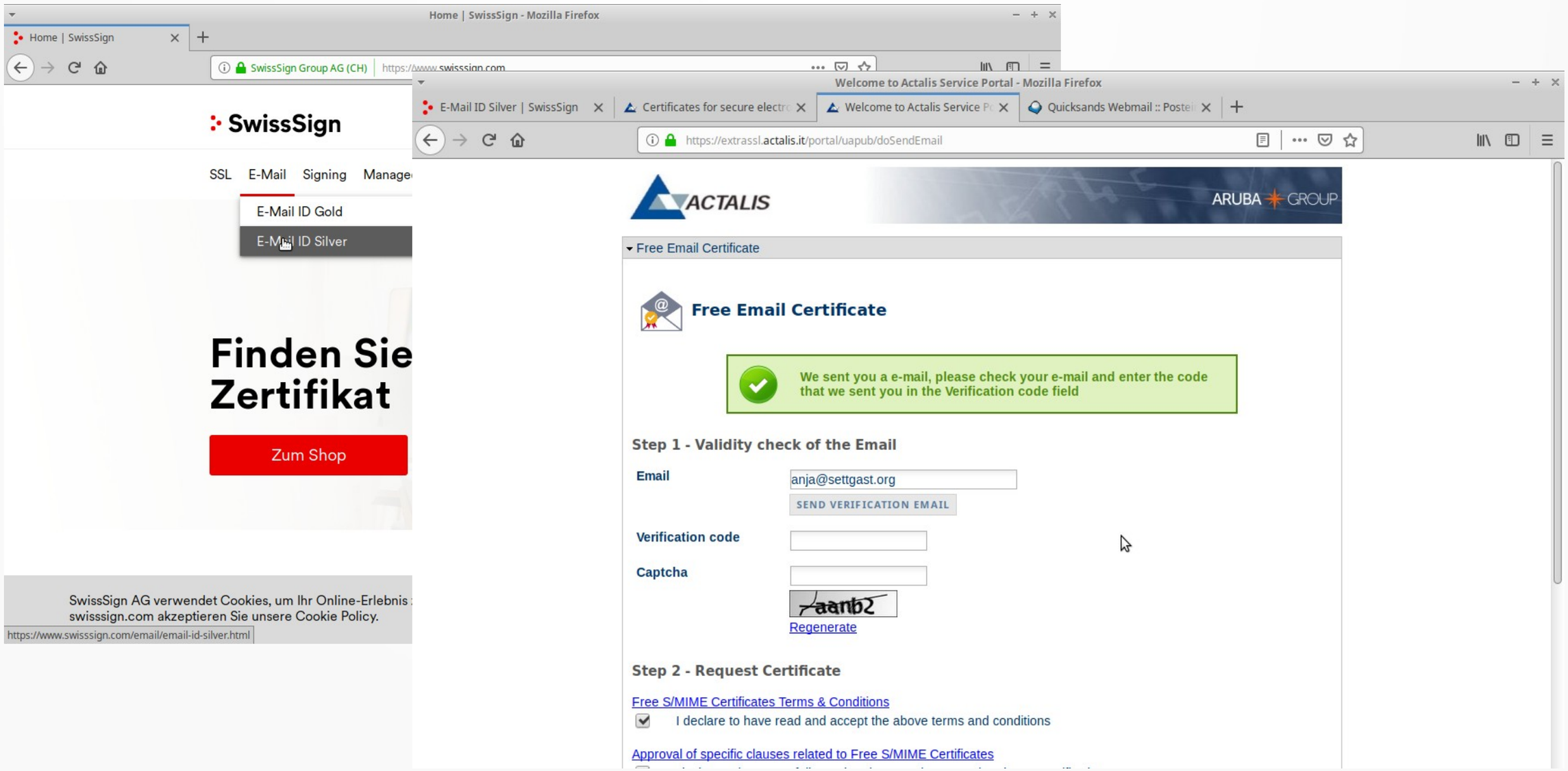
Welche Verfahren gibt es?

- 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

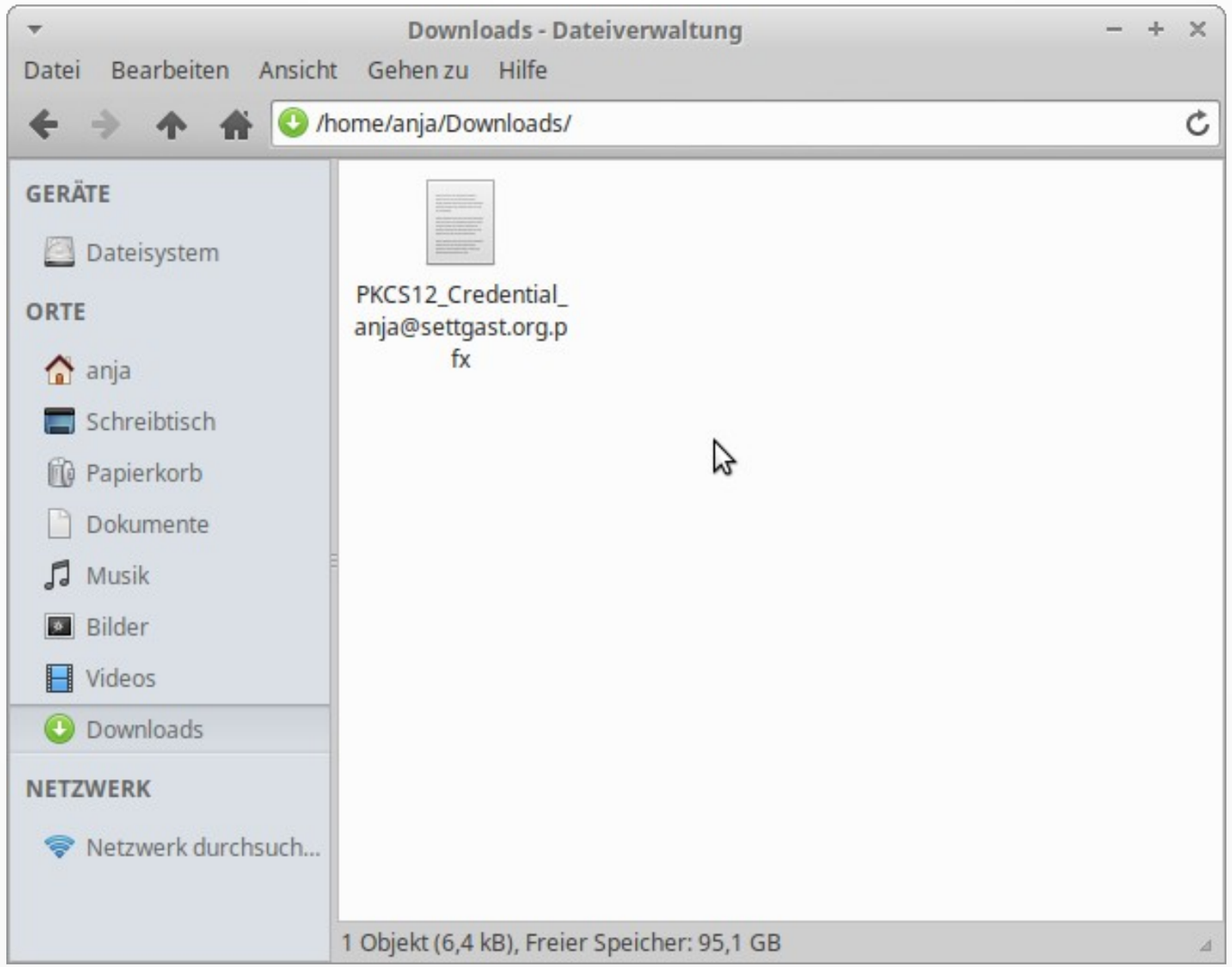
S/MIME

- 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



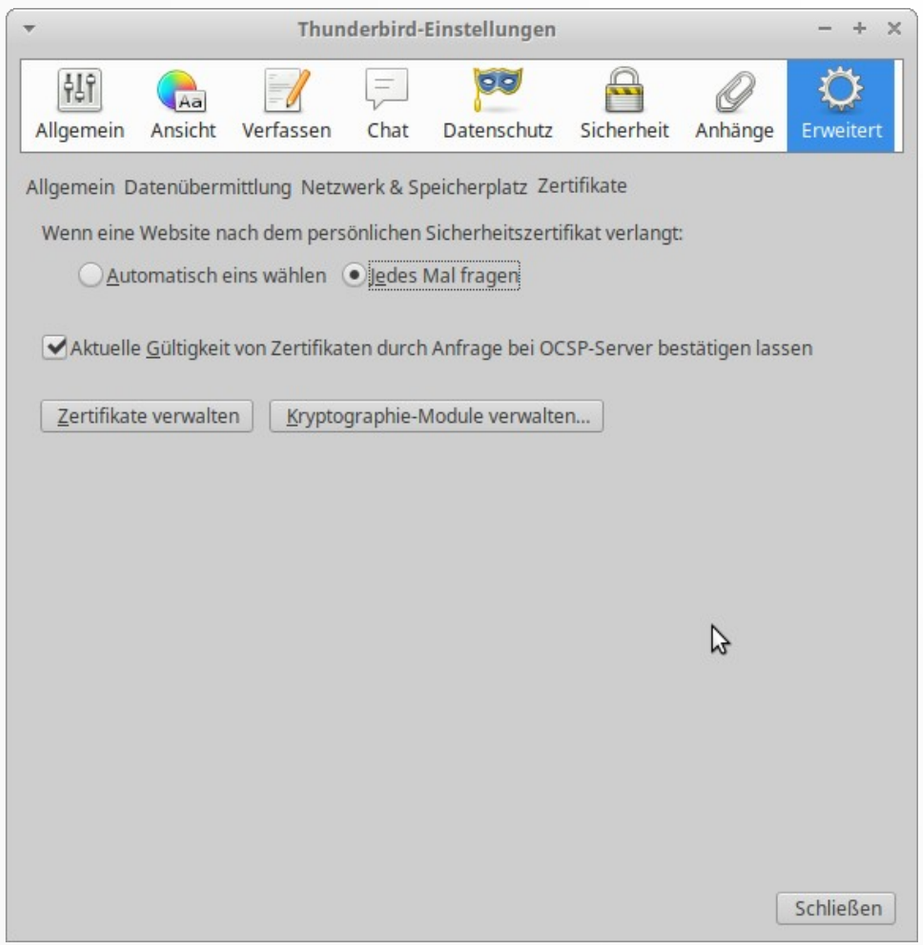
Ergebnis: Zertifikatsdatei

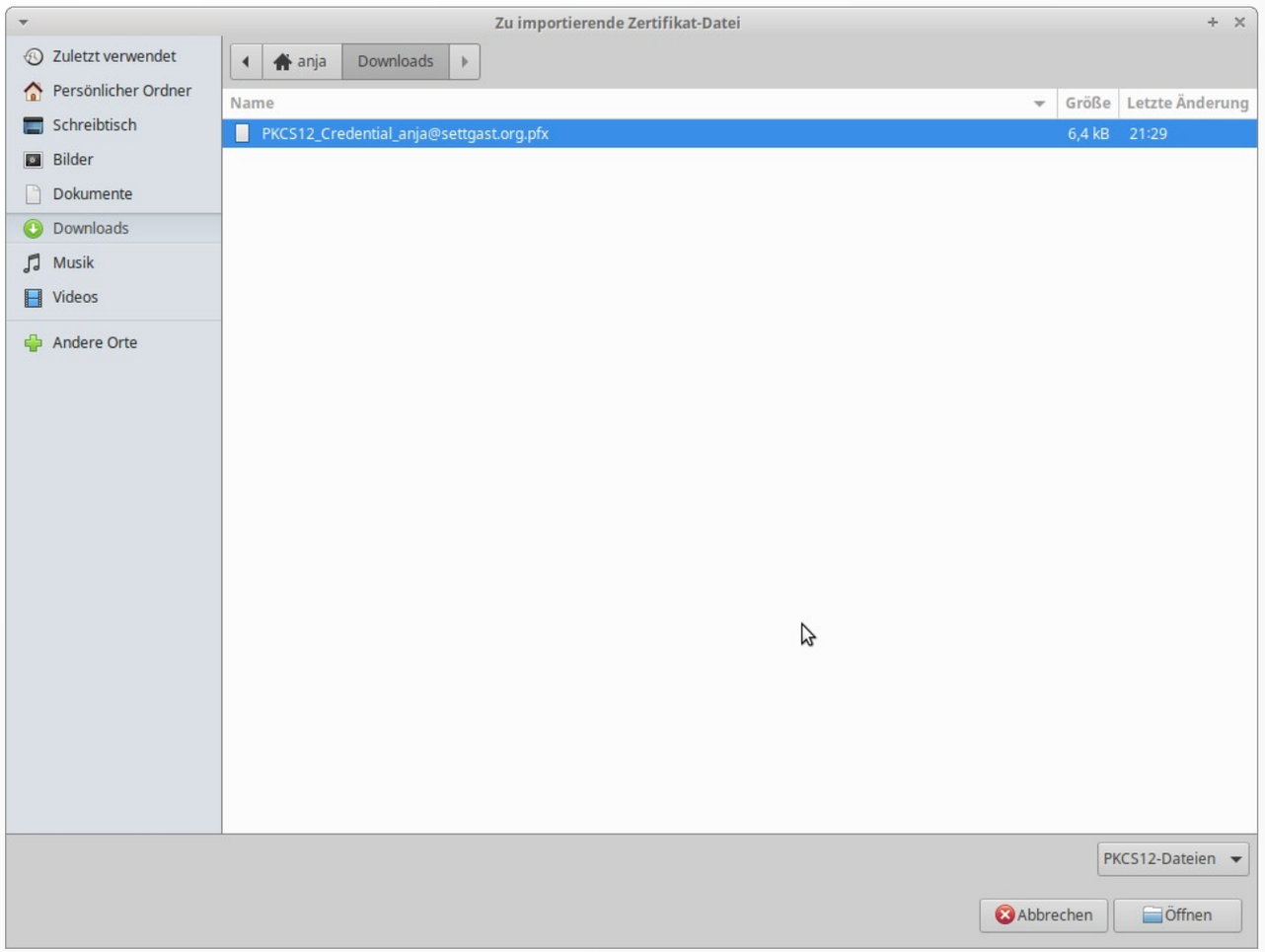


Was muss Anja einrichten?

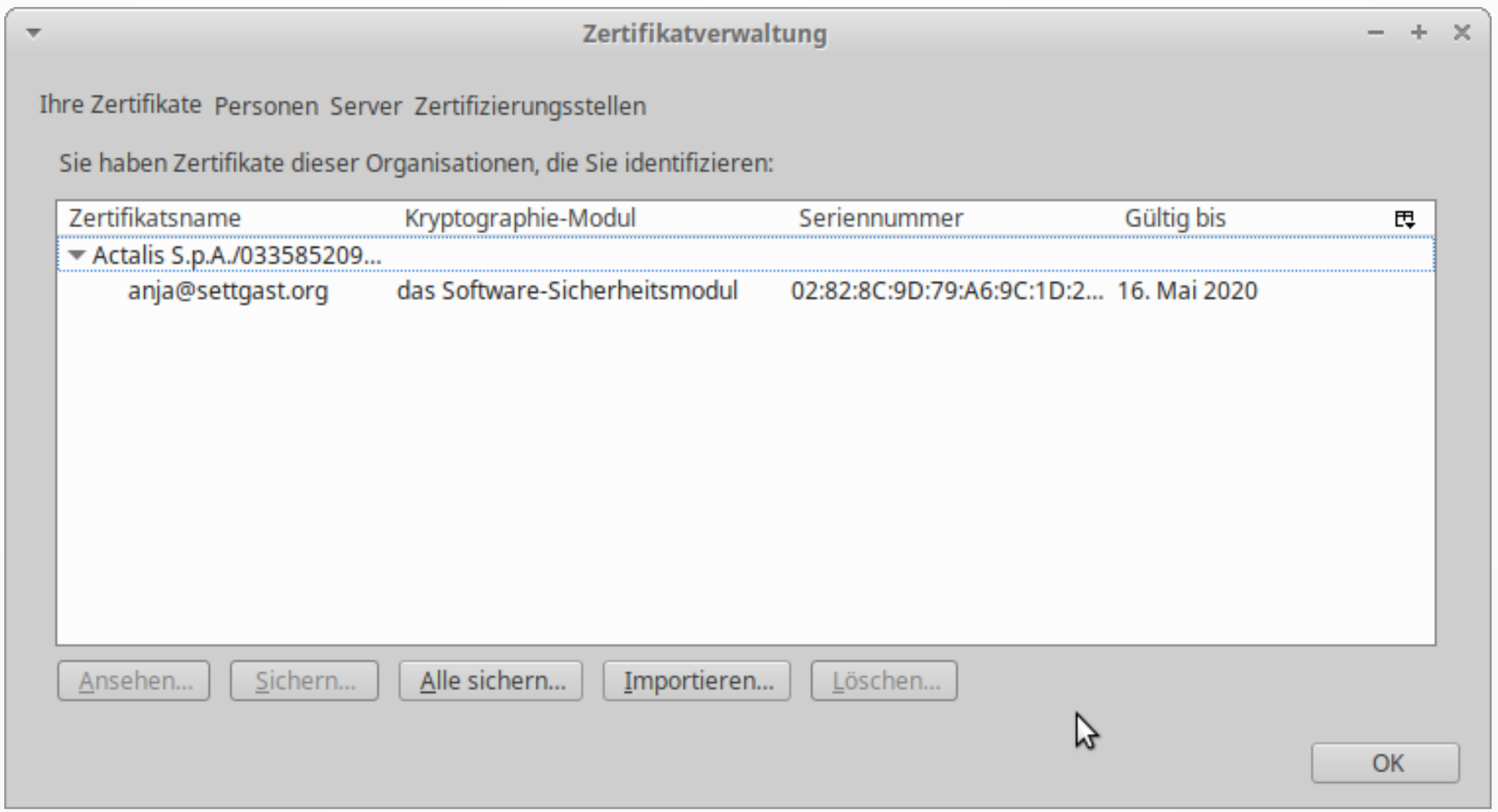
- Zertifikat in Thunderbird importieren und im Account konfigurieren

Zertifikate verwalten

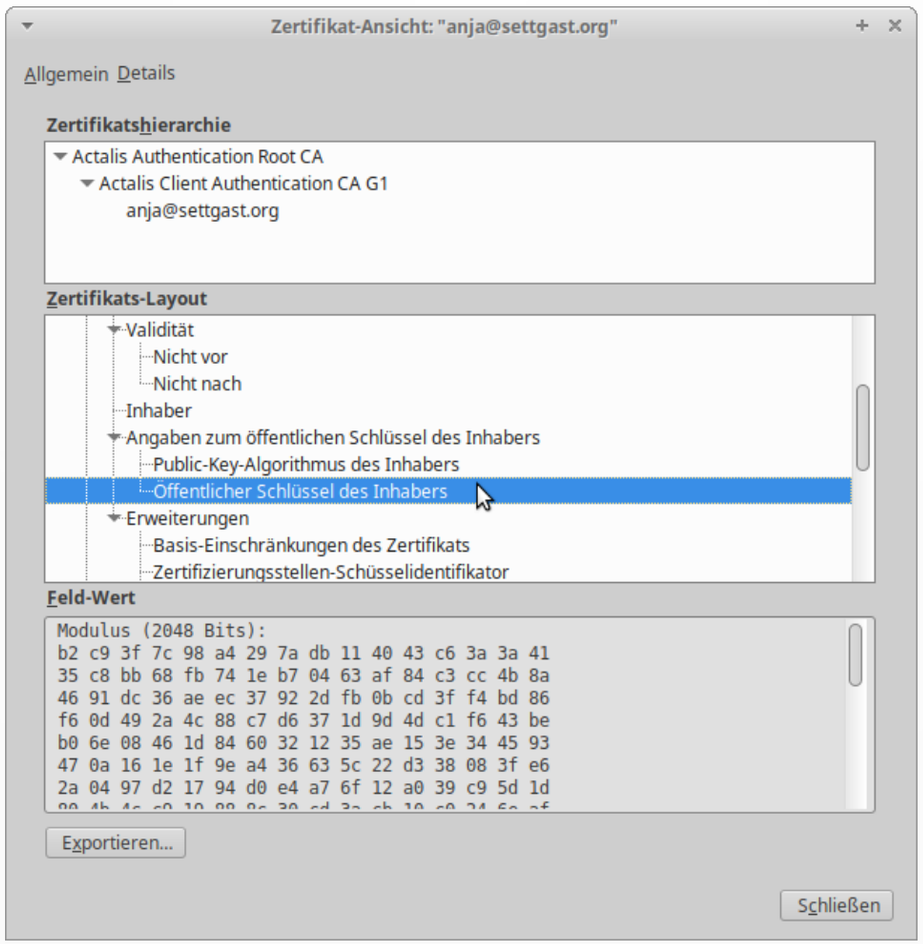




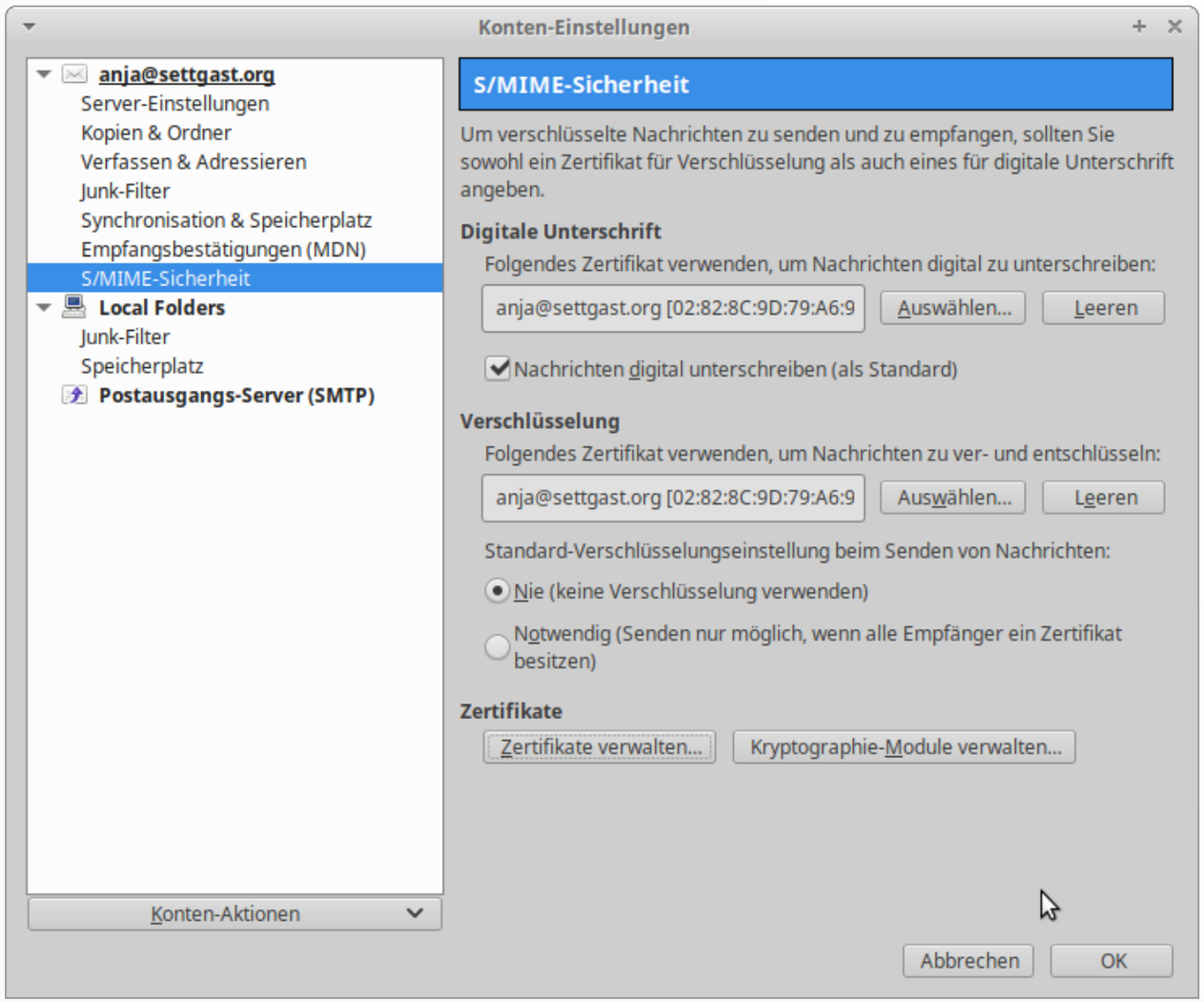
Zertifikat importiert



Was steckt im Zertifikat?



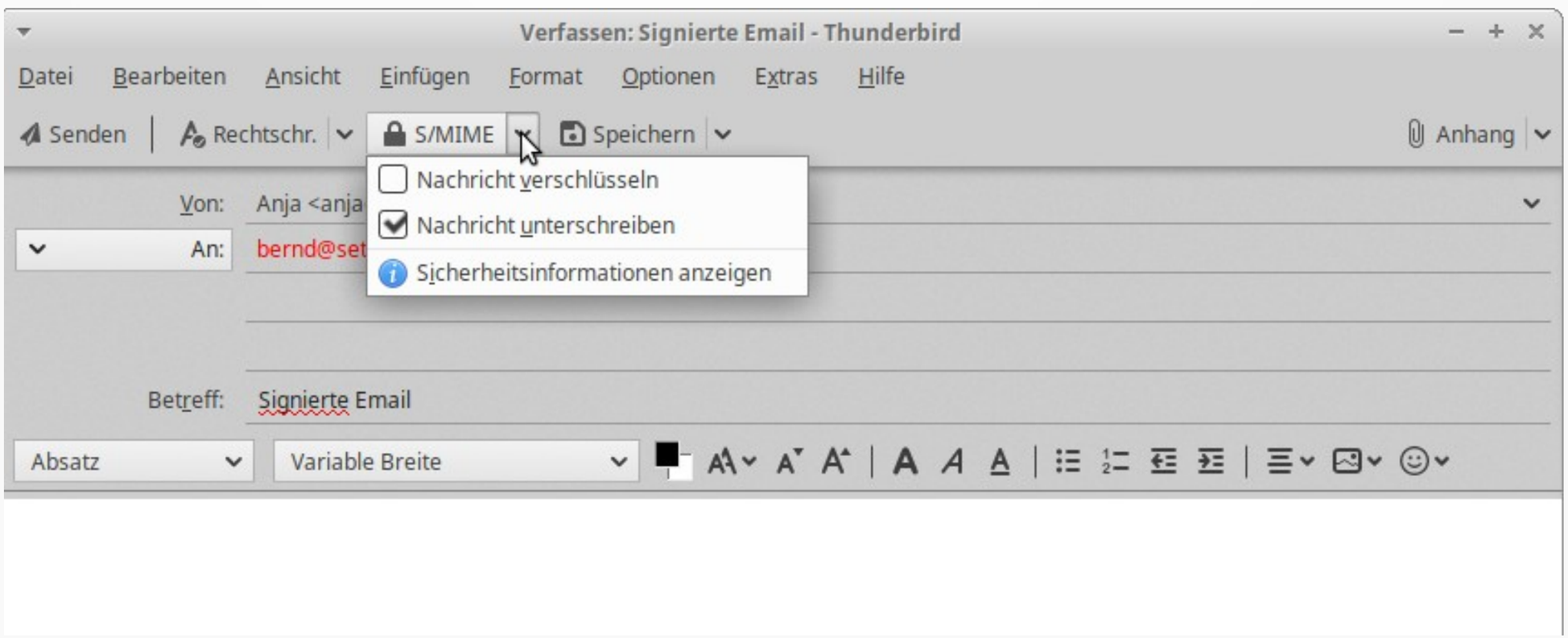
Email-Konto konfigurieren



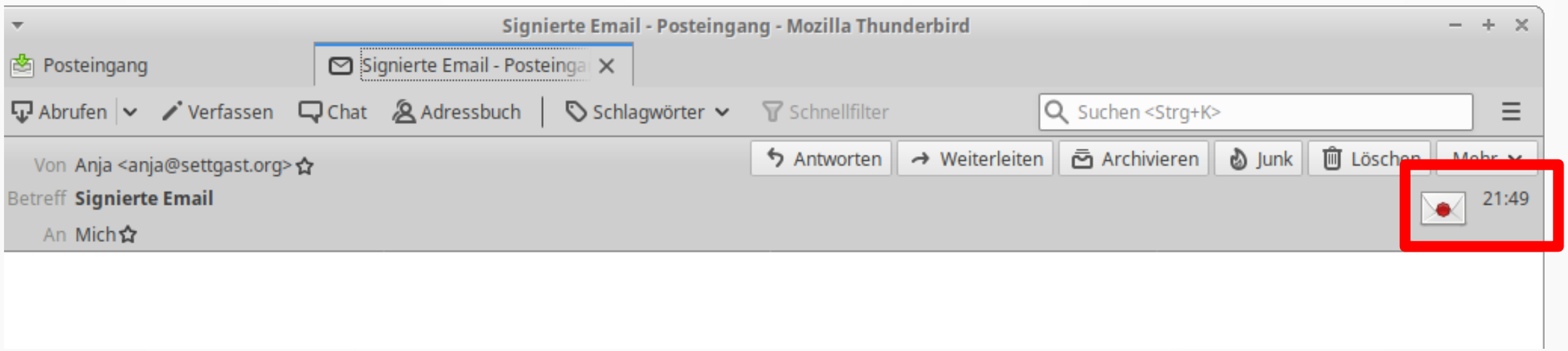
- Zertifikat zum Signieren auswählen
- „Nachrichten digital unterschreiben (als Standard)“ auswählen
- Zertifikat für Verschlüsselung auswählen

Was braucht Bernd?

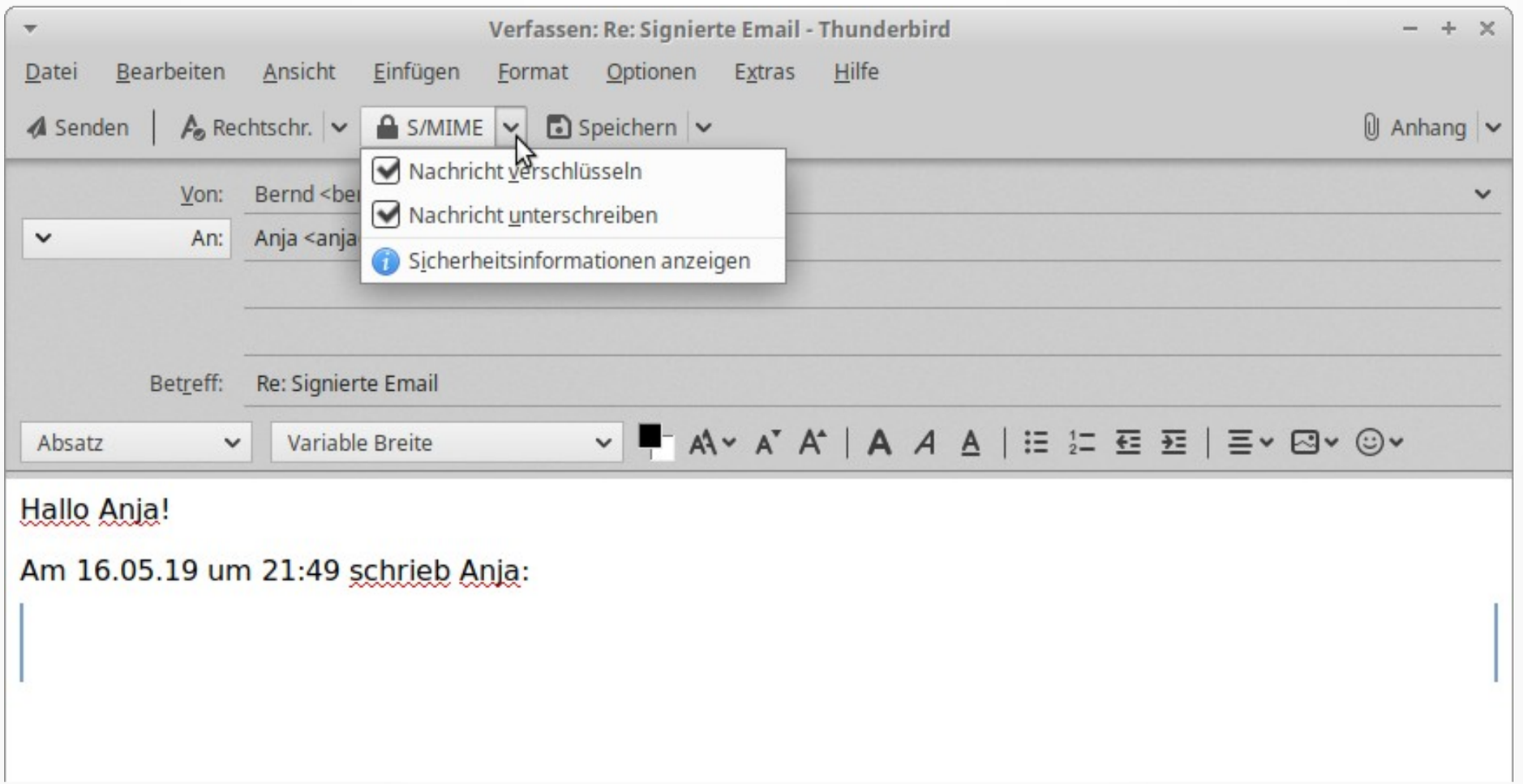
- Öffentlichen Schlüssel von Anja, im Zertifikat enthalten
- Anja schickt signierte Email an Bernd



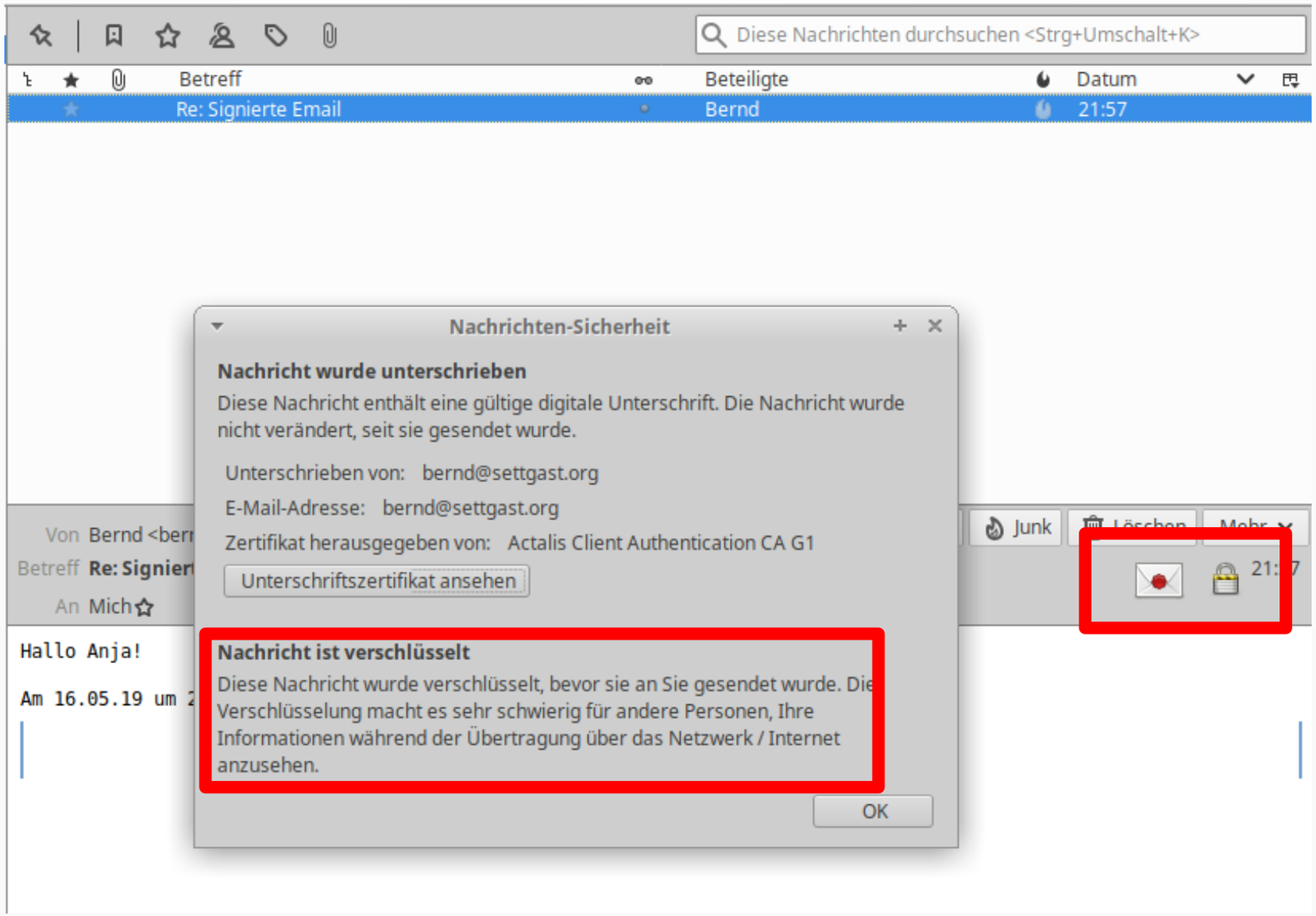
So sieht das bei Bernd aus



Bernd schickt signierte und verschlüsselte Email an Anja



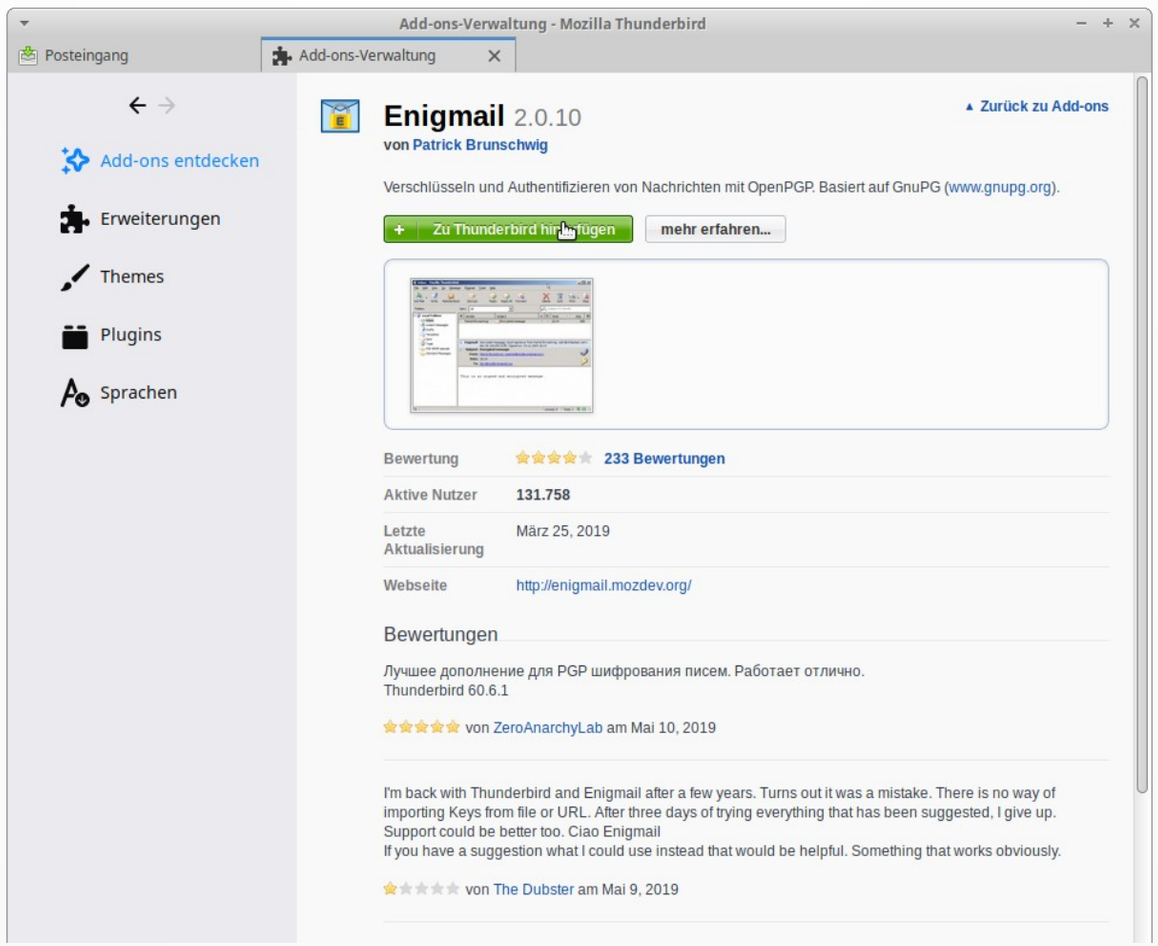
So sieht das bei Anja aus



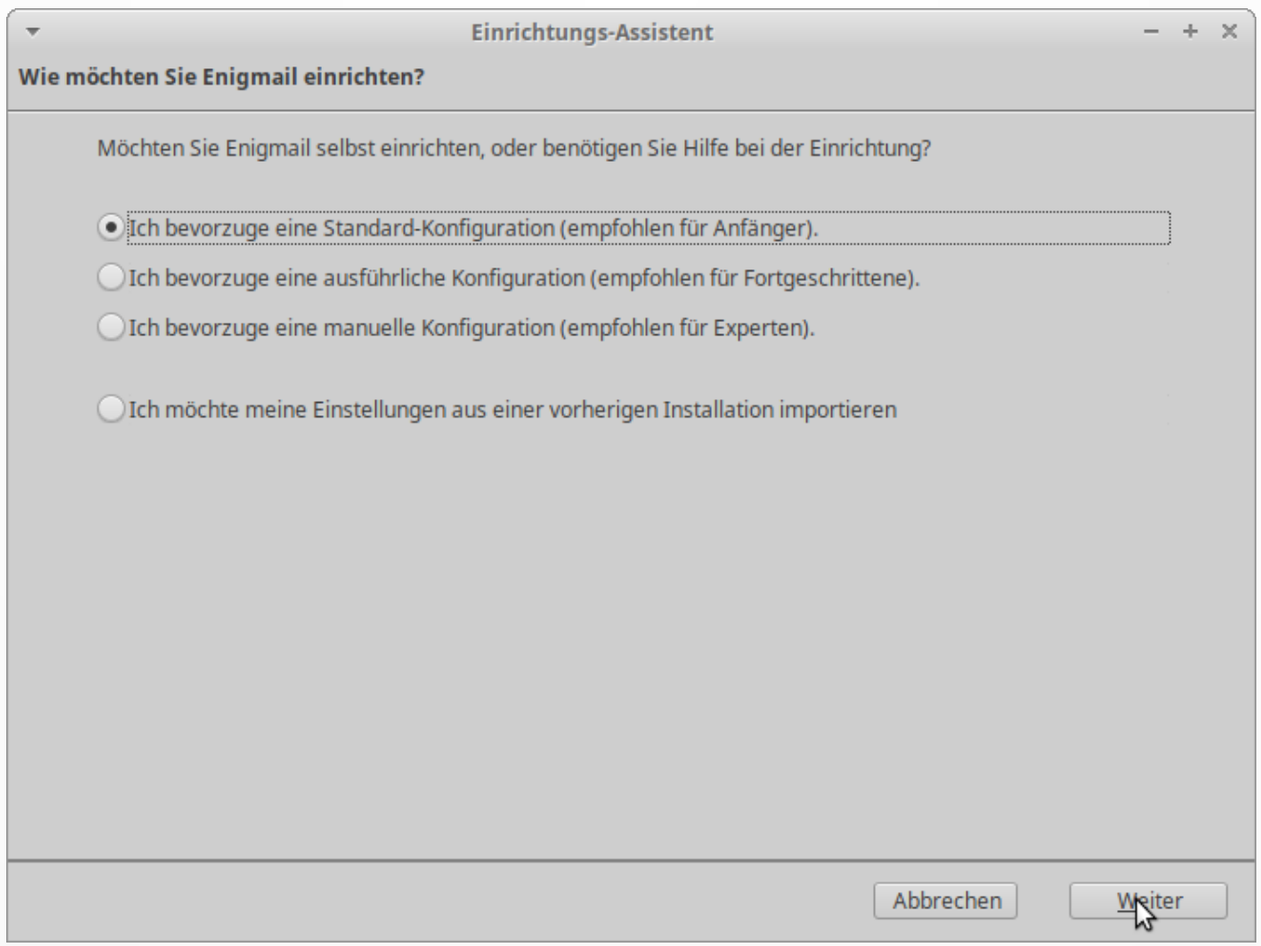
PGP

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

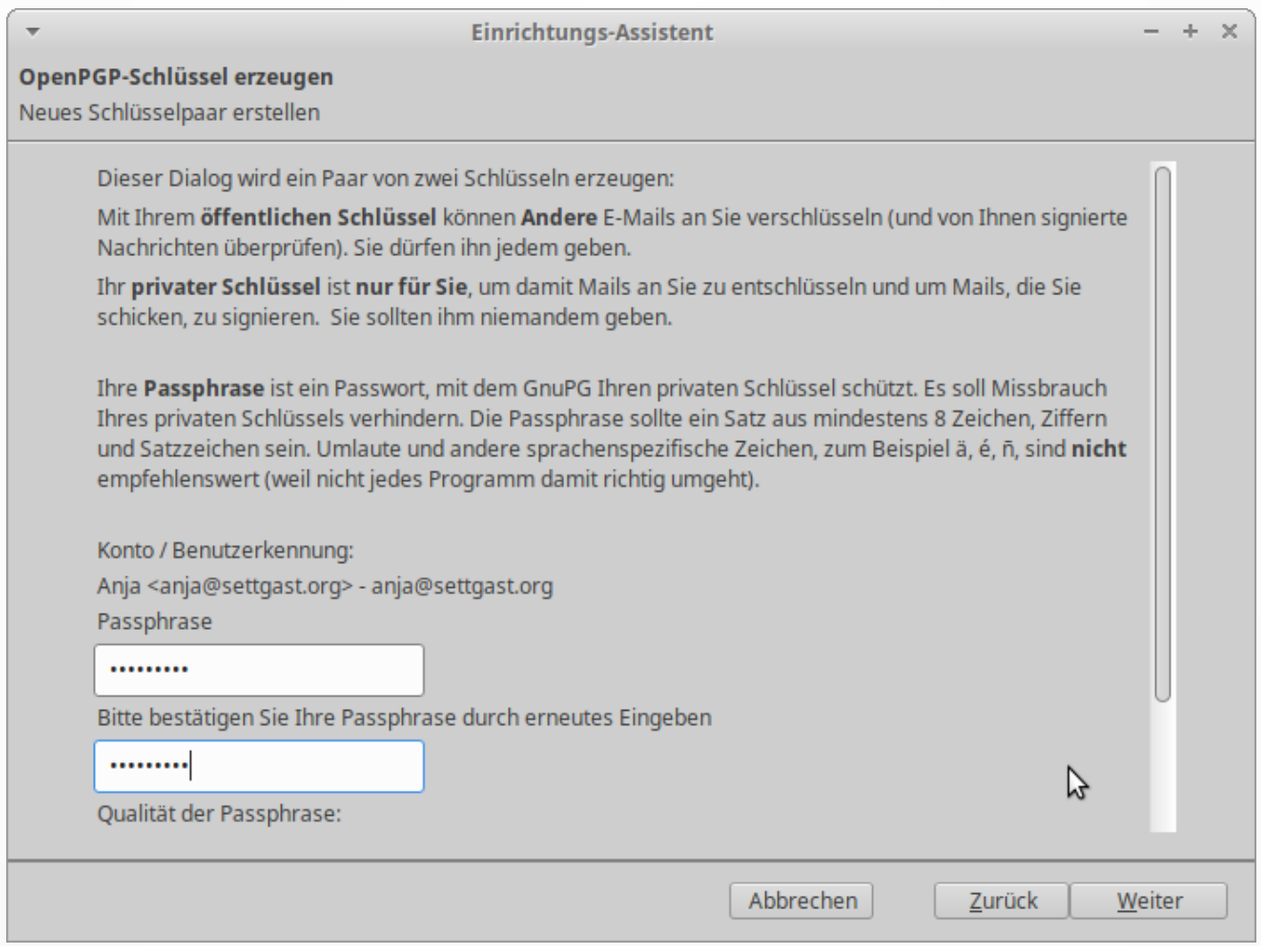
Was braucht Anja?



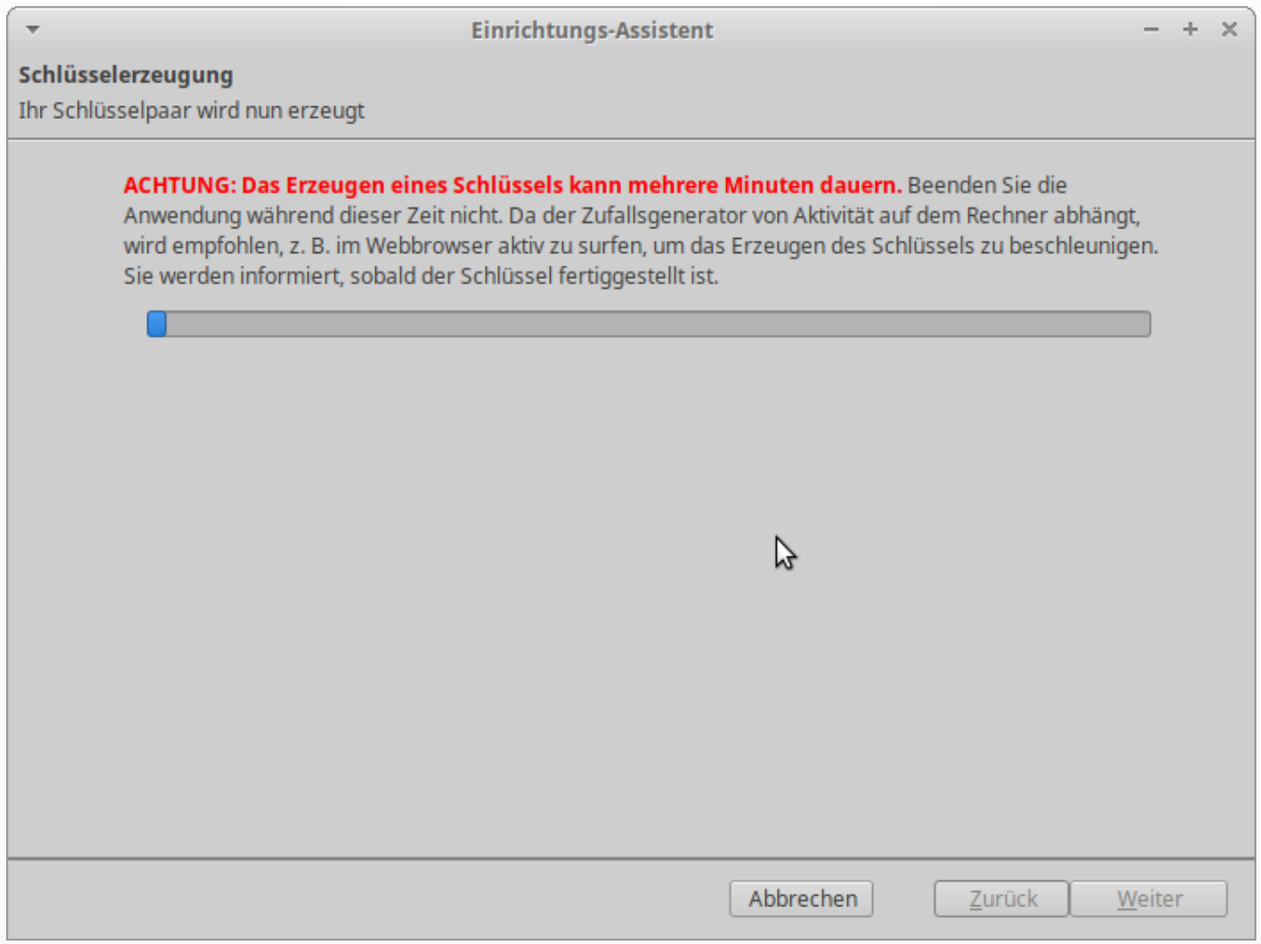
Wie richtet sie es ein?



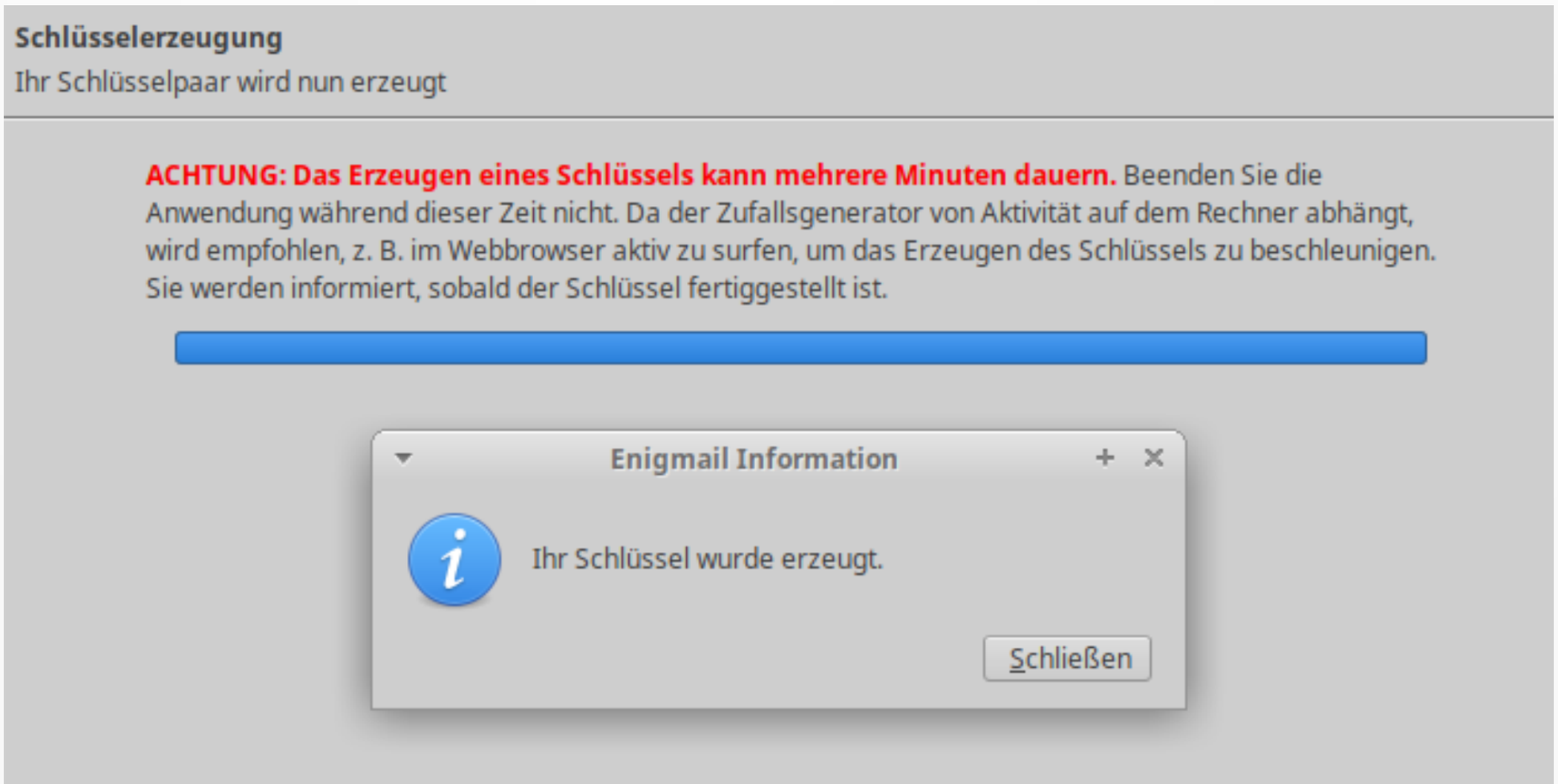
Schlüsselpaar erzeugen



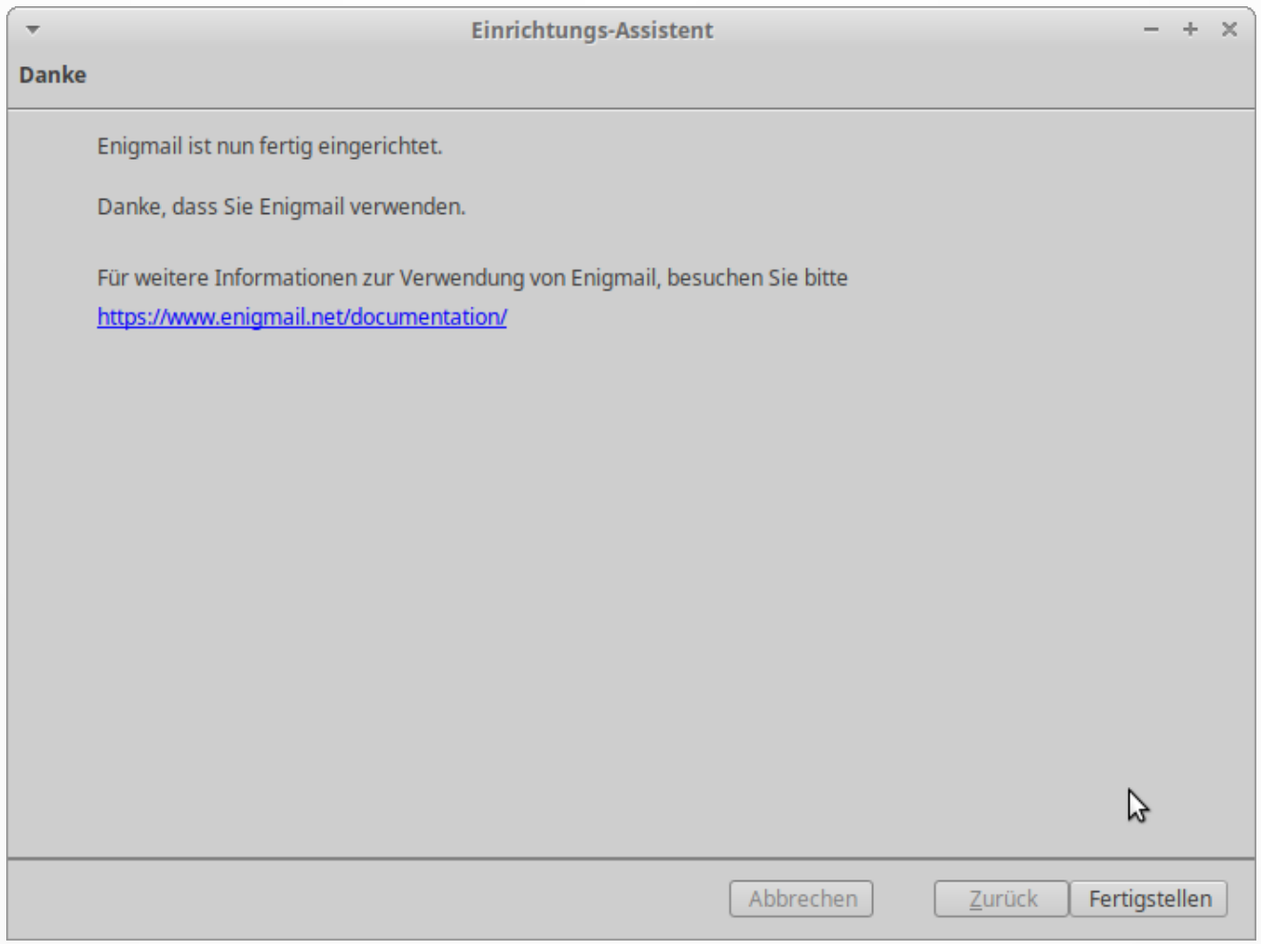
Schlüsselpaar erzeugen



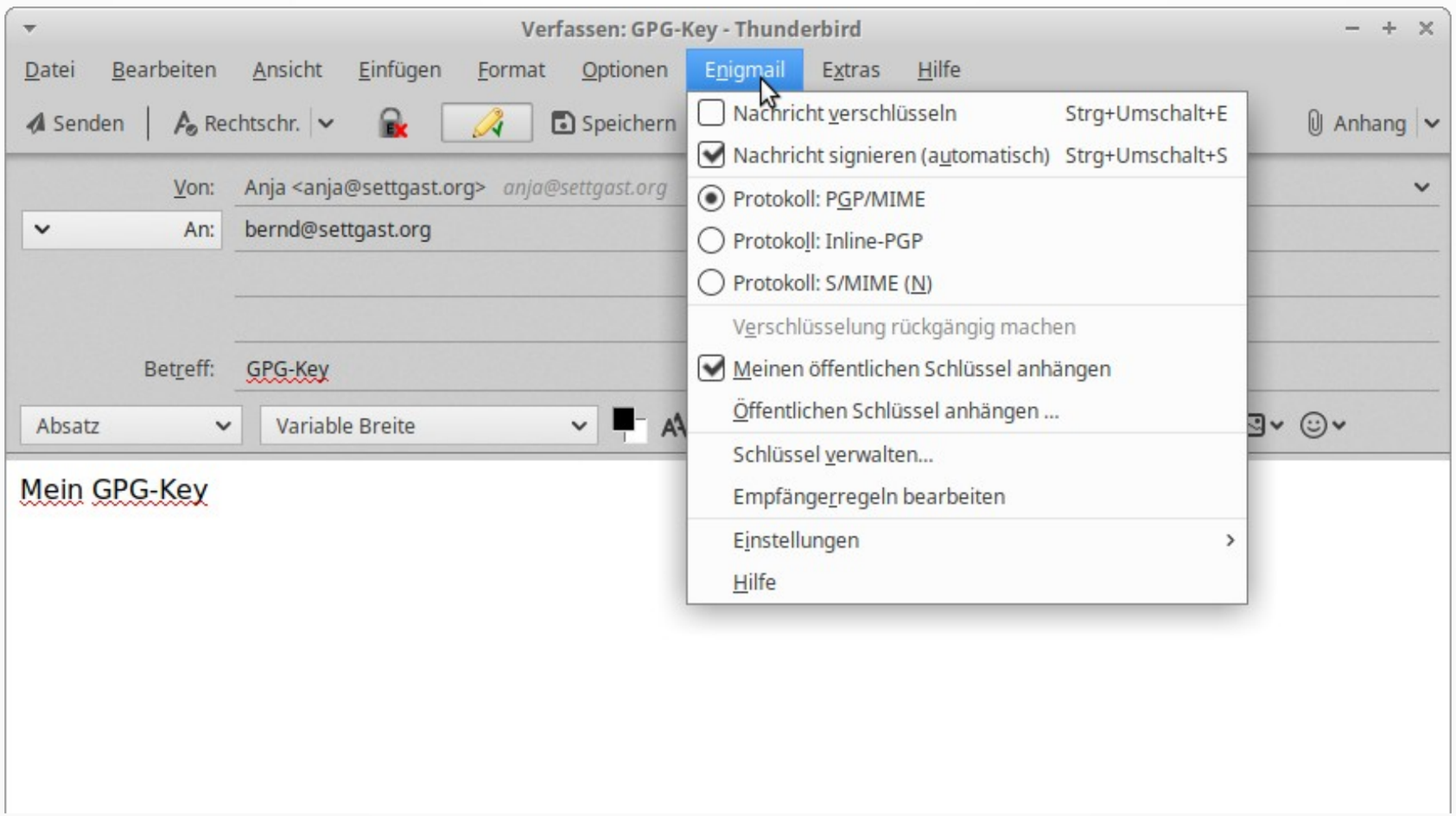
Schlüsselpaar erzeugt



Einrichtung abgeschlossen

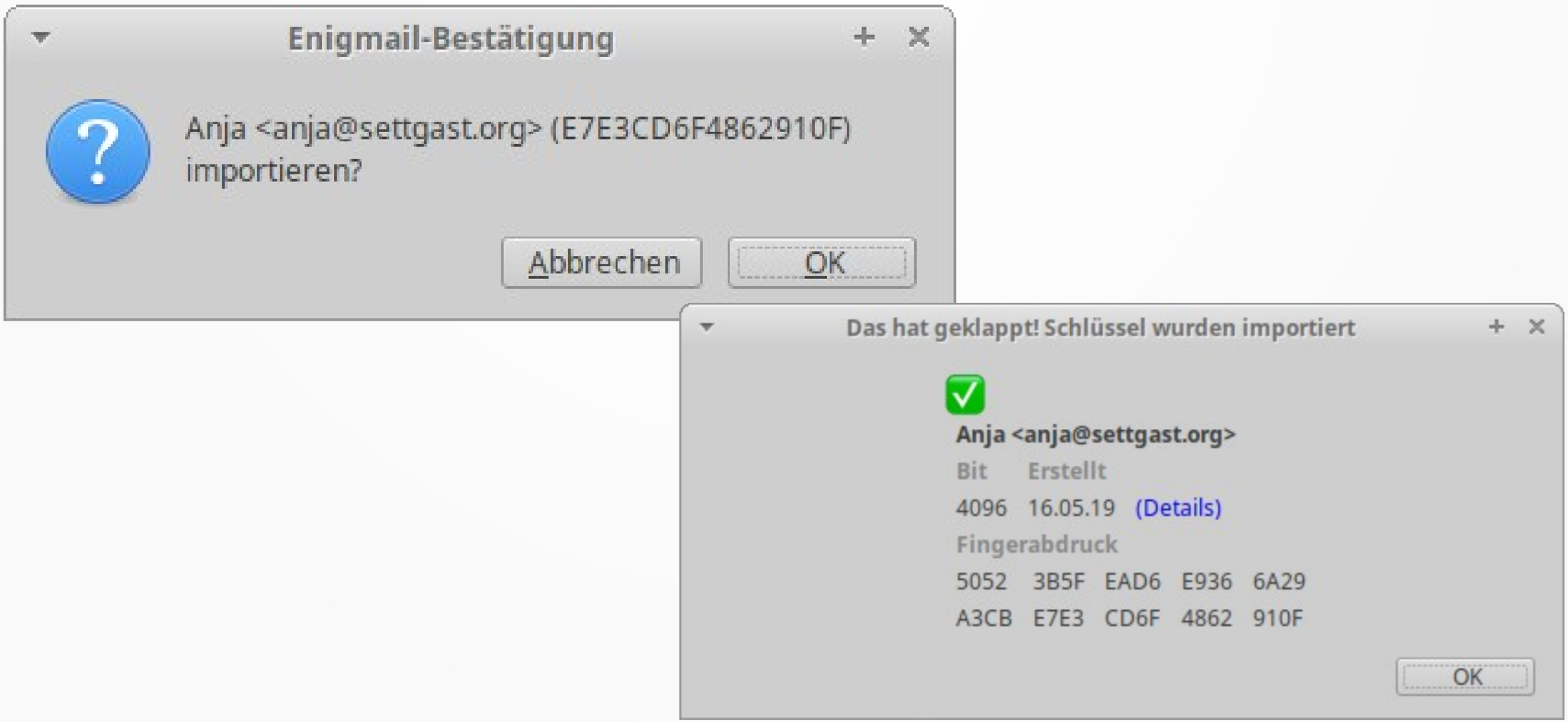


Anja schickt GPG-Key an Bernd

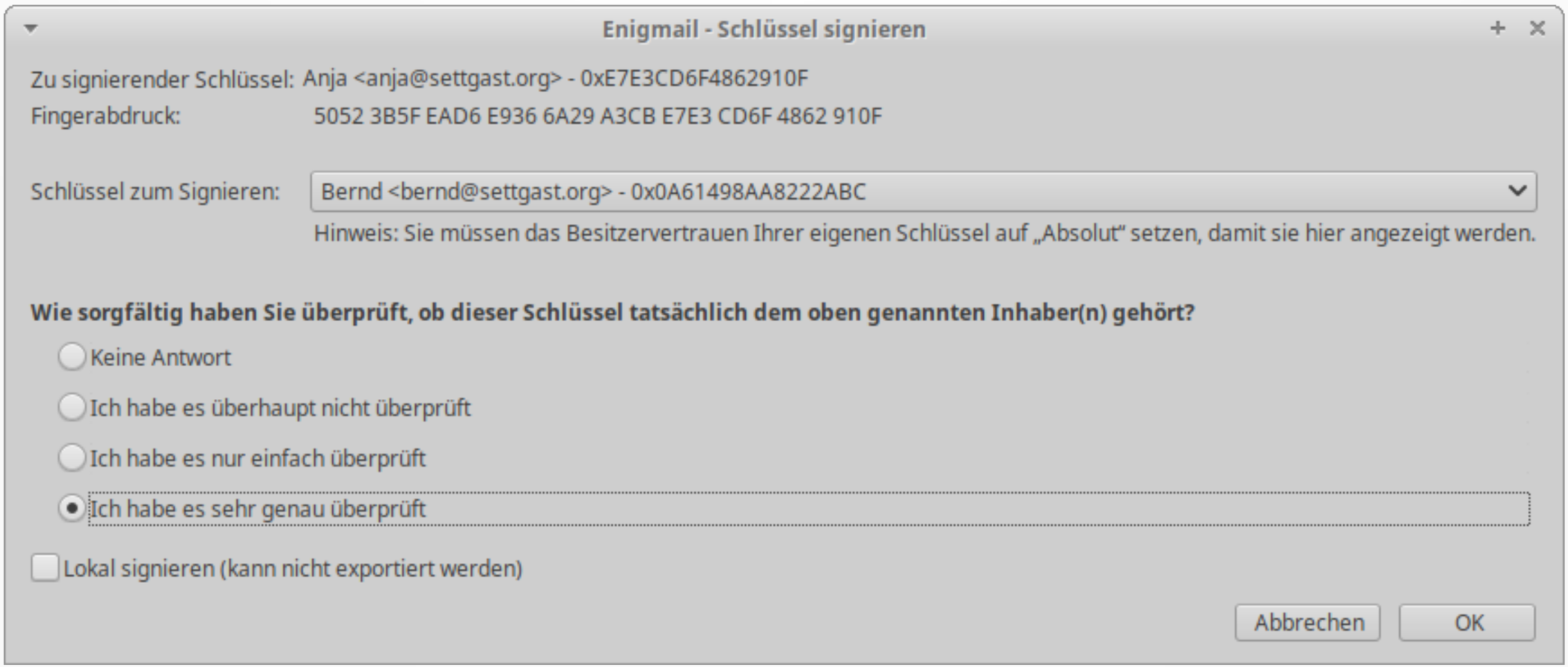


So sieht das bei Bernd aus

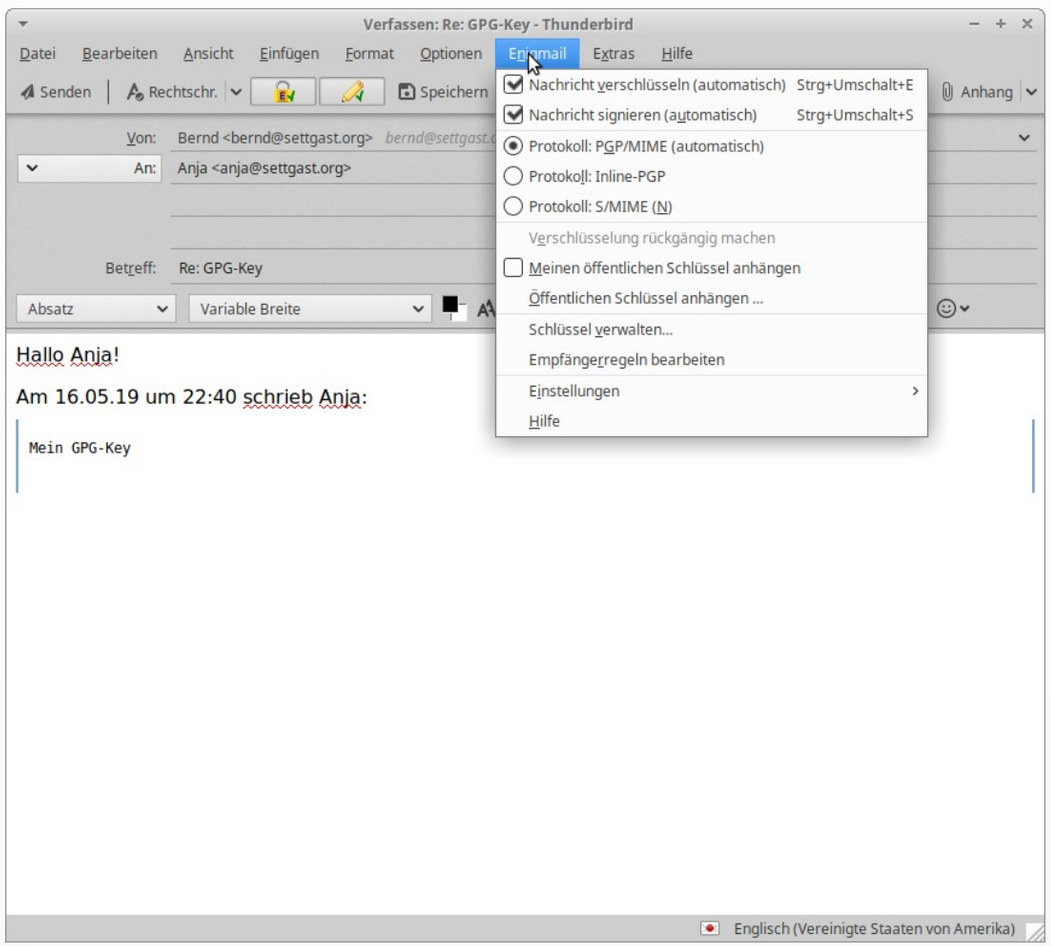
Bernd prüft Schlüssel von Anja



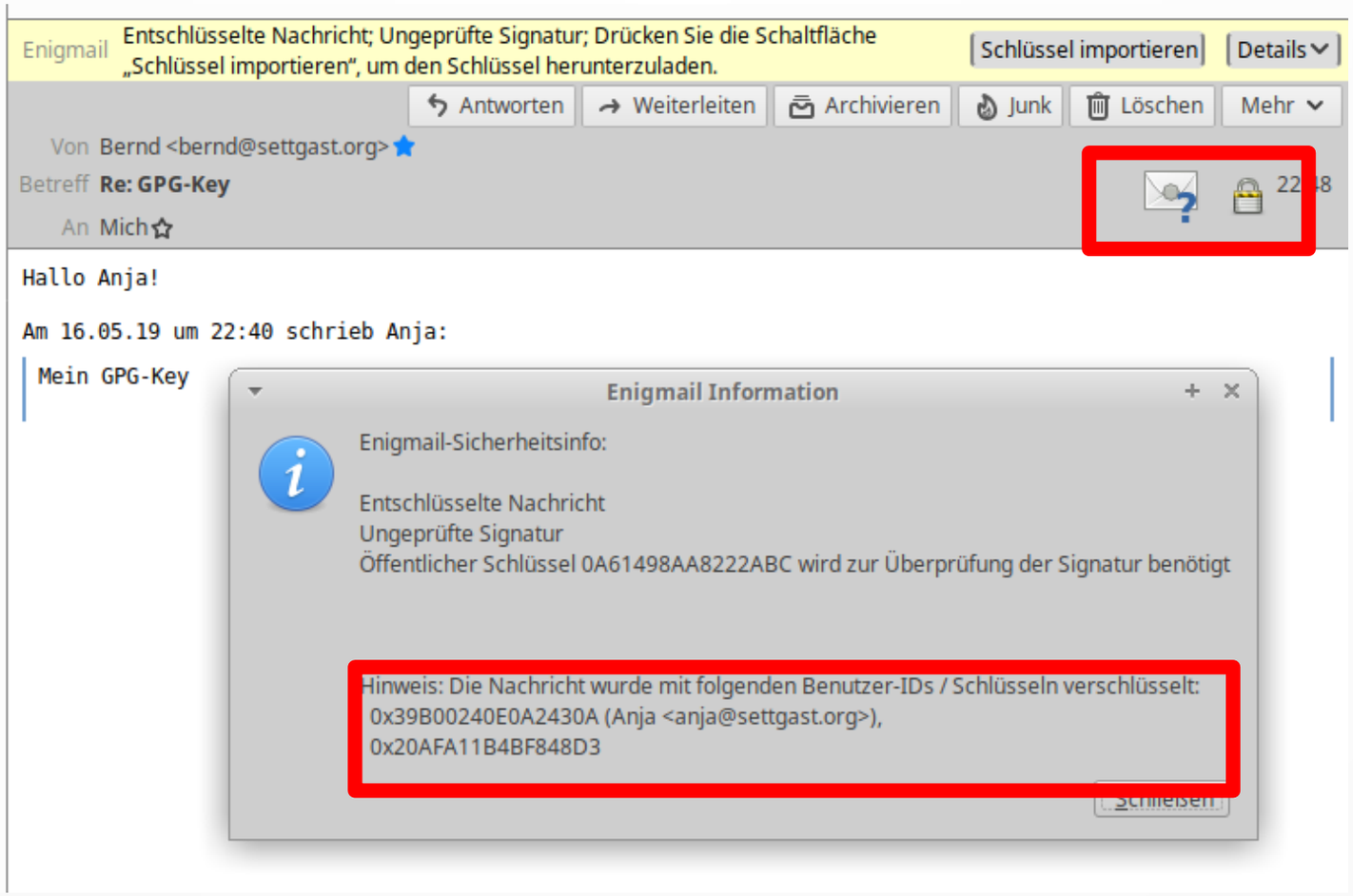
Bernd prüft Schlüssel von Anja



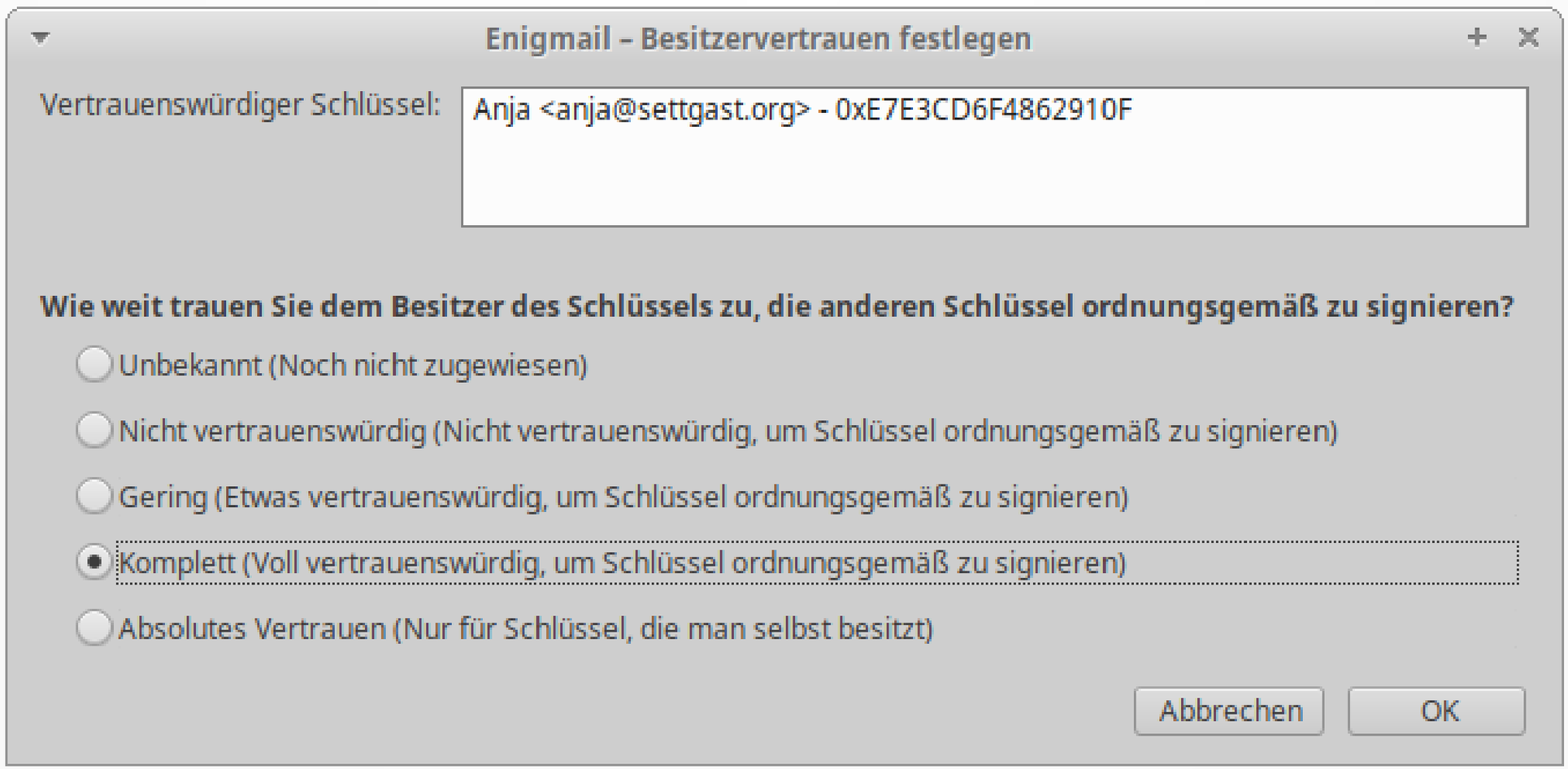
Bernd schickt signierte und verschlüsselte Email



So sieht das bei Anja aus



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



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