1. Politischer Hintergrund
2. Ein bisschen Theorie
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
3. Praxis
    1. Installation eines E-Mail-Programms
    2. Erstellen von Schlüsseln
4. Weiterführendes

1. Hintergrund

- 2013: Edward Snowden

Bankrotterklärung des Innenministers

Friedrich ruft zum Verschlüsseln auf

Die Innenpolitiker der CSU sagen, dass die Bürger beim Datenschutz nicht auf den Nationalstaat hoffen dürfen. Sie sollen ihre Daten selber schützen.

Kommt etwas ins Schwimmen: Bundesinnenminster Friedrich. Bild: dpa

BERLIN *taz* | Als Konsequenz aus der Spähaffäre hat Bundesinnenminister Hans-Peter Friedrich (CSU) die Bürger zum Verschlüsseln ihrer Onlinekommunikation aufgerufen. „Wir werden dafür sorgen, dass noch mehr Menschen in Deutschland ihre eigene Kommunikation noch sicherer machen“, sagte Friedrich nach einer Sondersitzung des Parlamentarischen Kontrollgremiums zur Überwachung der Geheimdienste (PKGr). Als Mittel nannte er Verschlüsselungstechnik und Virenabwehrprogramme.

http://www.taz.de/!120071/

PGP: bekanntes, sicheres Verschlüsselungsverfahren

EU-Parlament entwickelt Paket für „PGP-artige“ Software und verweist in der Zwischenzeit auf Office, 7zip und PDF

von Anna Biselli am 27. April 2015, 12:33 in EU / 15 Kommentare

Letzte Woche habe wir darüber berichtet, dass im Europaparlament seit Beginn der

DG ITEC Generaldirektion Innovation und technologische Unterstützung

DG ITEC rät, sich mit der „internen Verschlüsselung“ von Office, 7zip und PDF in der Zwischenzeit Abhilfe zu verschaffen. Dafür müsse man jedoch ein Passwort austauschen – mündlich. Wir können uns leider bereits vorstellen, wie das über ungesicherte Telefonleitungen passiert.

https://netzpolitik.org/2015/eu-parlament-entwickelt-paket-fuer-pgp-artige-software-und-verweist-in-der-zwischenzeit-auf-office-7zip-und-pdf/

EU-Kommission hat weiterhin „Bedenken“ zu Verschlüsselung und plant Gespräche mit Internetdienstleistern

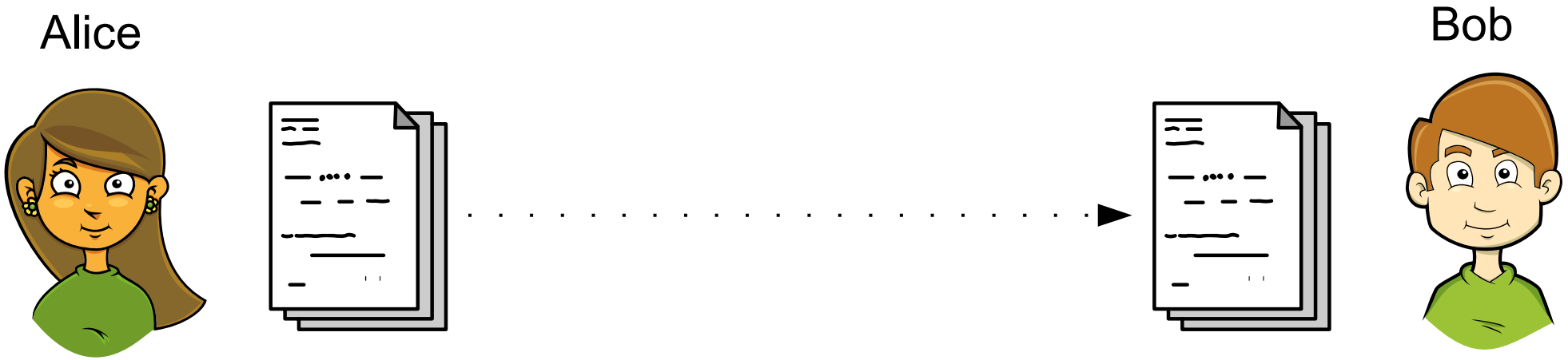
von Matthias Monroy am 29. April 2015, 14:00 in Überwachung / 14 Kommentare

Die EU-Kommission findet die Nutzung von Verschlüsselungswerkzeugen weiterhin problematisch. Dies geht aus der gestern veröffentlichten „Europäischen Sicherheitsagenda“ hervor. Demnach hätten Strafverfolgungsbehörden „Bedenken in Bezug auf die neuen Verschlüsselungstechniken“. Damit knüpft die Kommission an Statements des EU-Anti-Terror-Koordinators Gilles de Kerchove an. Der hatte im Januar in einer Wunschliste gefordert, Internet- und Telekommunikationsanbieter zum Einbau von

Sieht in Verschlüsselungstechniken das „größte

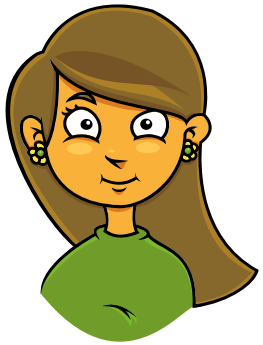
2. Theorie

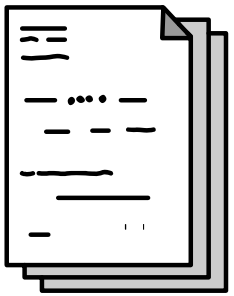
Symmetrische Verschlüsselung



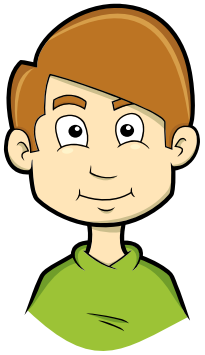
Symmetrische Verschlüsselung

Alice



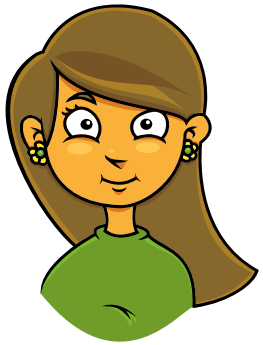


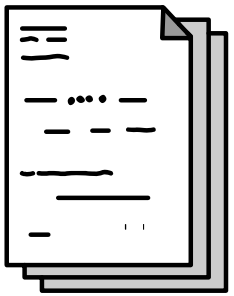
Bob



Symmetrische Verschlüsselung

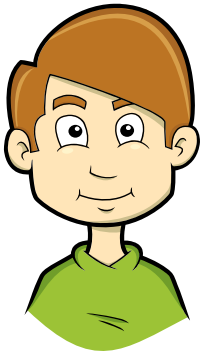
Alice



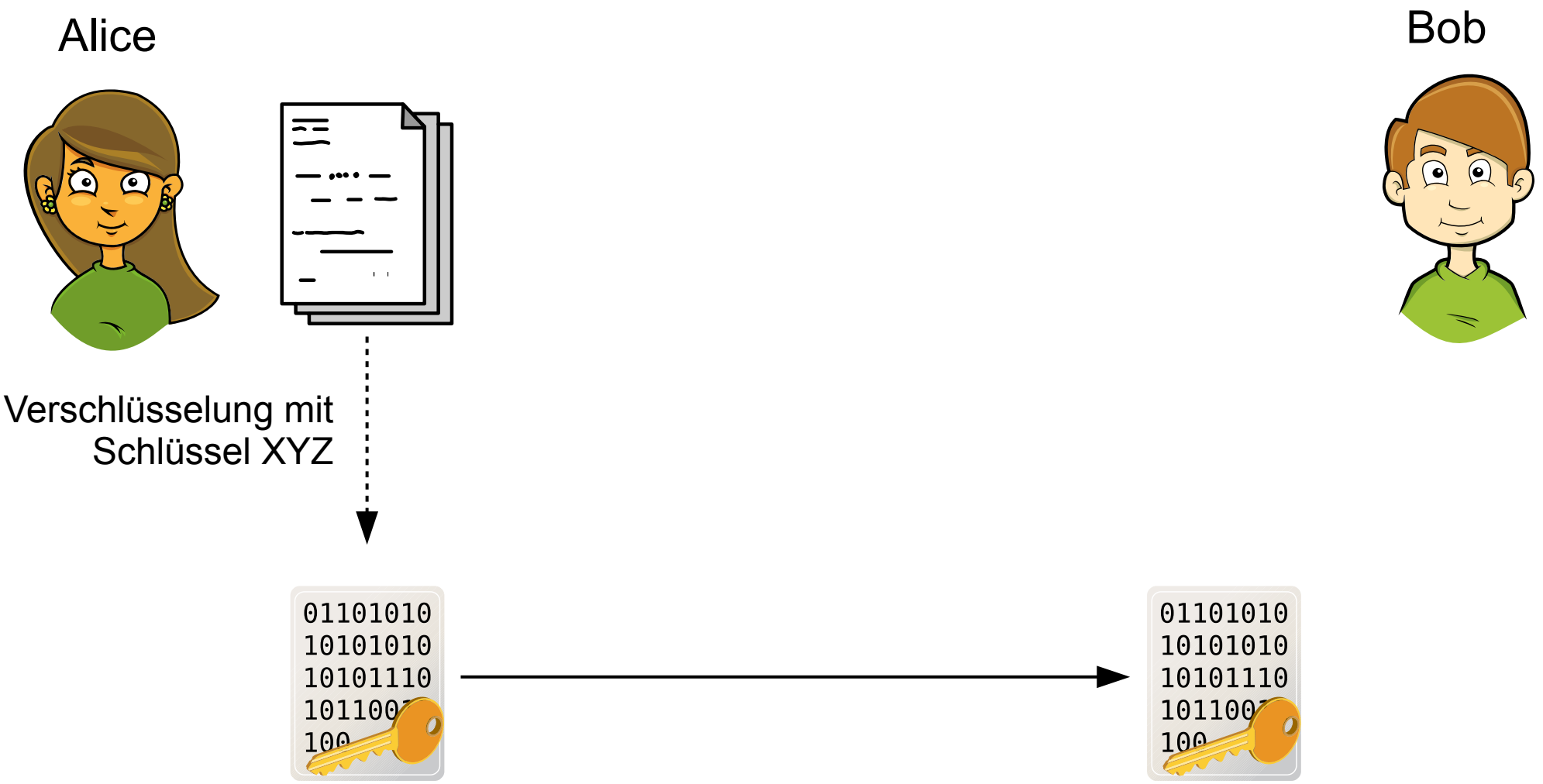


Verschlüsselung mit
Schlüssel XYZ

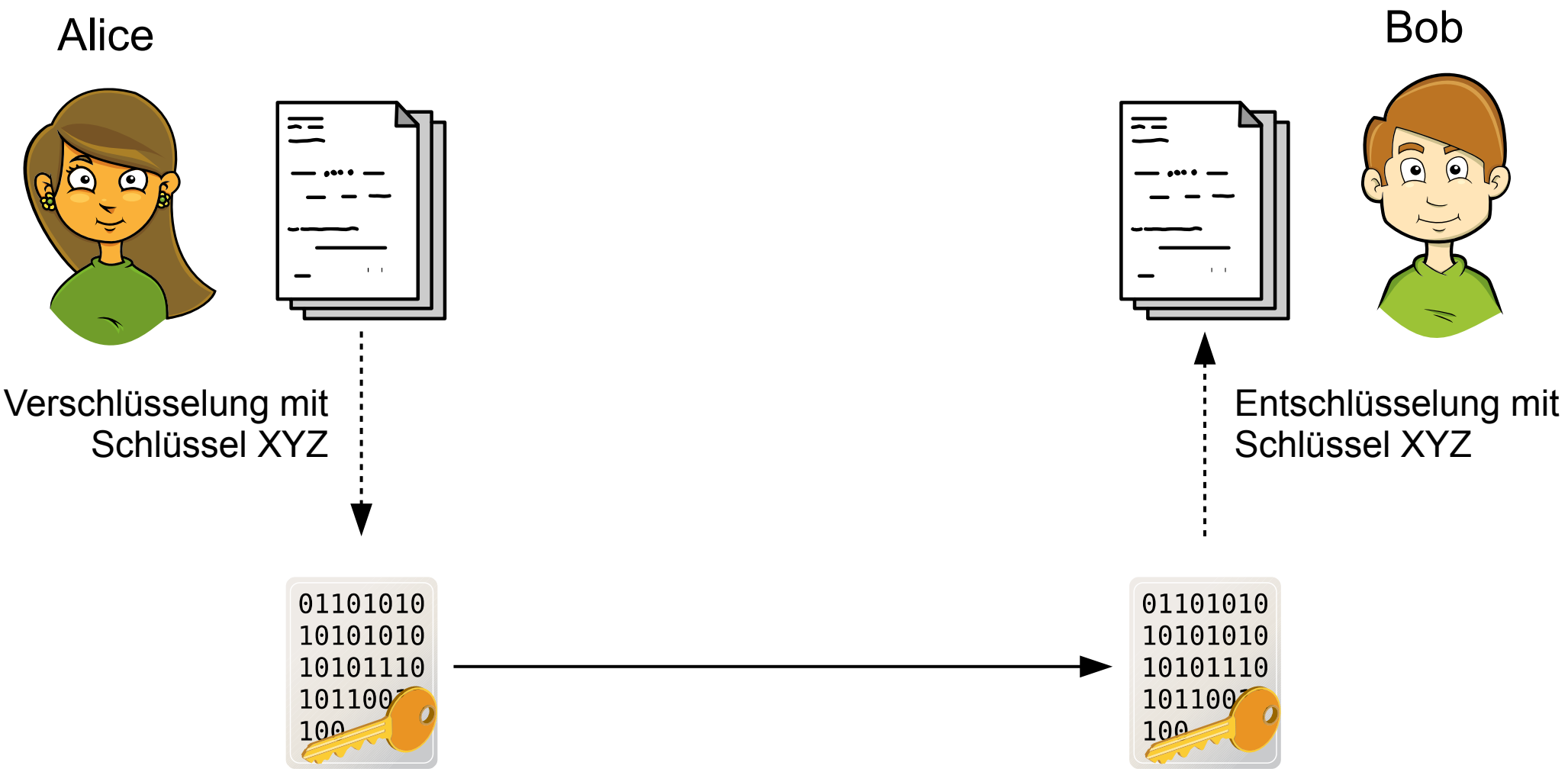
Bob



Symmetrische Verschlüsselung



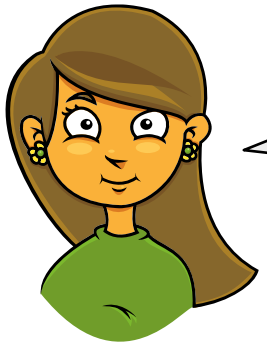
Symmetrische Verschlüsselung



Problem

Problem

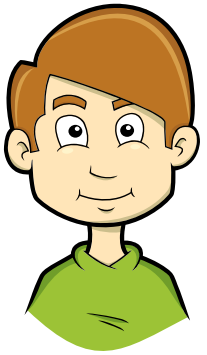
Alice



Hallo Bob, der geheime Schlüssel ist XYZ!

Okay, danke!

Bob



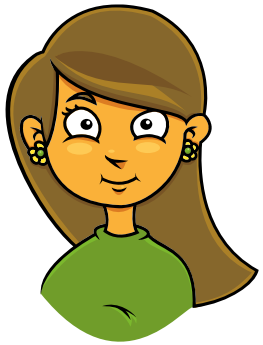
Ver schlüsselung mit Schlüssel XYZ

Ent schlüsselung mit Schlüssel XYZ

Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

Alice



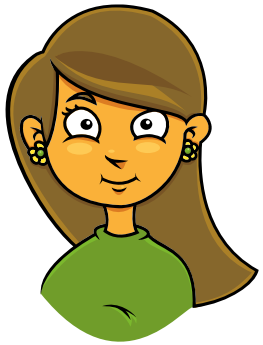
private key (Alice)

Öffentlich

public key (Alice)

Asymmetrische Verschlüsselung

Alice



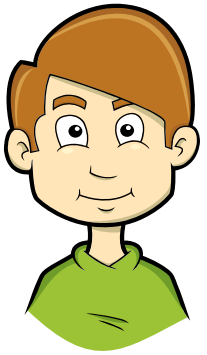
private key (Alice)

Öffentlich

public key (Alice)

public key (Bob)

Bob



private key (Bob)

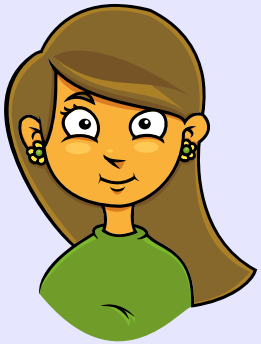
Alice an Bob: Verschlüsseln

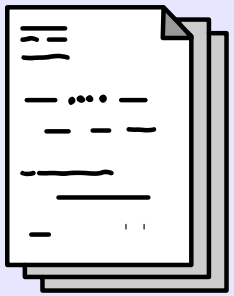
Privat

Öffentlich

Privat

Alice

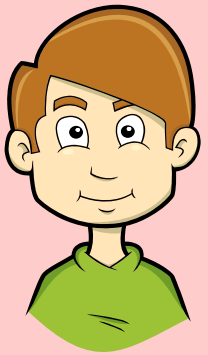




public key (Alice)

public key (Bob)

Bob



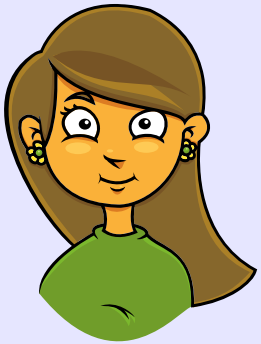
Alice an Bob: Versenden

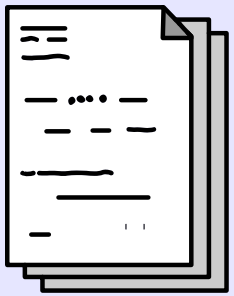
Privat

Öffentlich

Privat

Alice

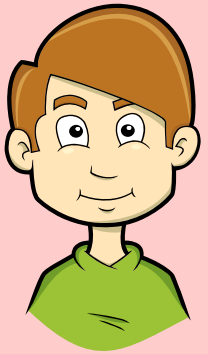


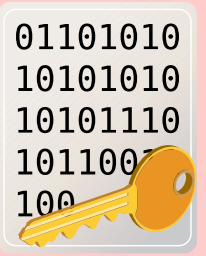


public key (Alice)

public key (Bob)

Bob





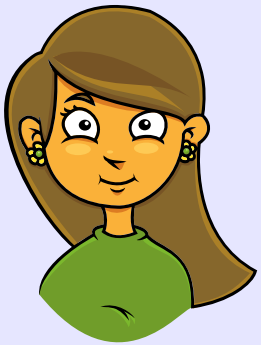
Alice an Bob: Entschlüsseln

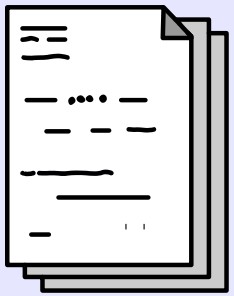
Privat

Öffentlich

Privat

Alice

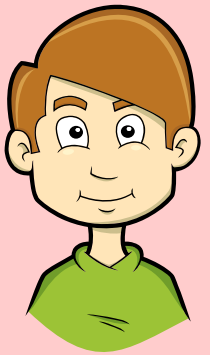




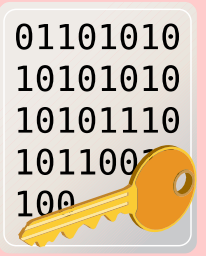
public key (Alice)

public key (Bob)

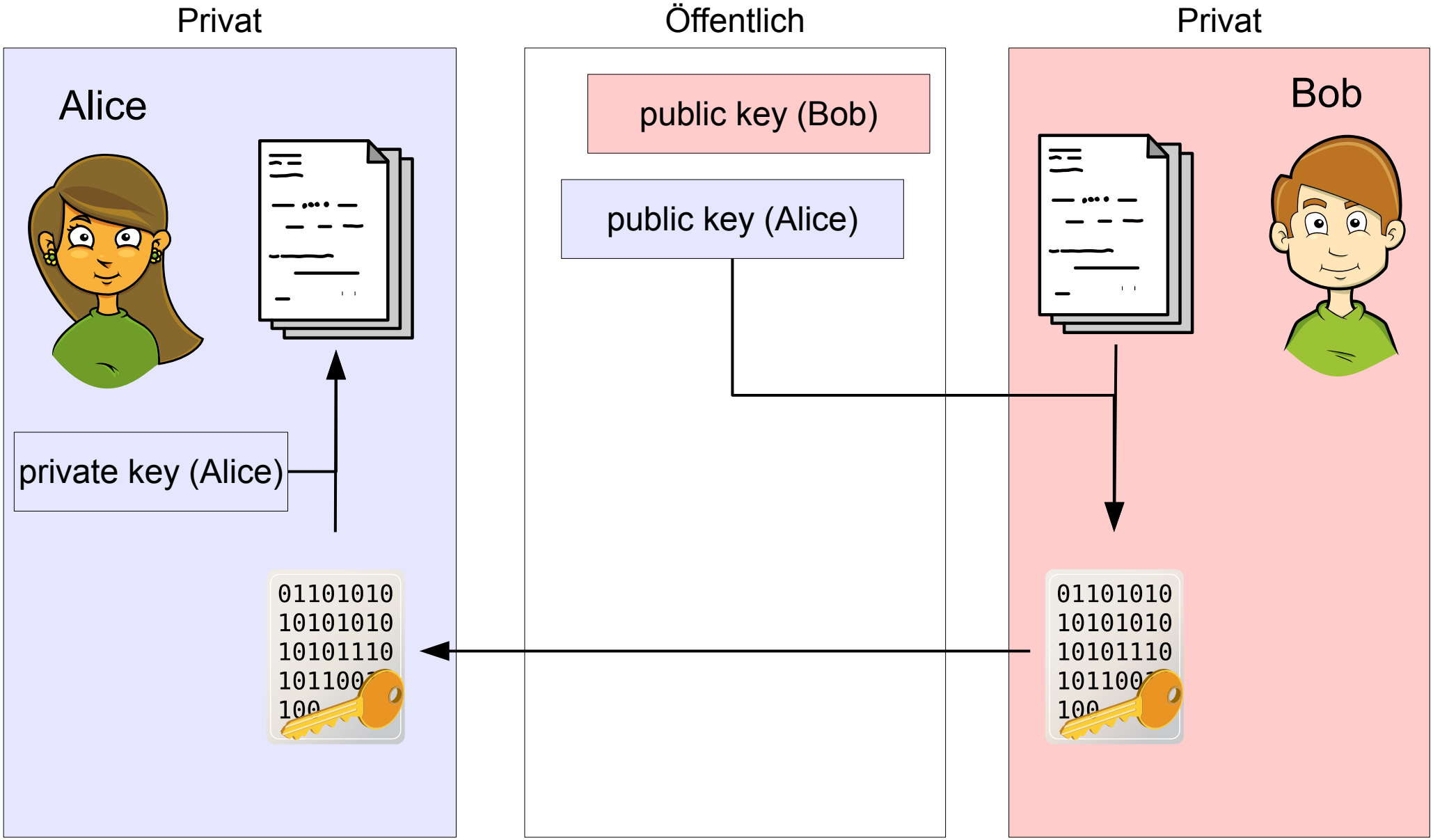
Bob



private key (Bob)



Bob an Alice


Privat
Öffentlich
Privat
Alice
Bob
public key (Bob)
public key (Alice)
private key (Alice)
01101010
10101010
10101110
01101010
10101010
10101110

Asymmetrische Verschlüsselung

- zwei Schlüssel pro Nutzer, einer davon geheim
- Jeder kann Nachricht an Bob verschlüsseln
- Nur Bob kann Nachricht an Bob entschlüsseln
- Man muss nichts Geheimes austauschen
- Privater Schlüssel muss geheim bleiben,
  also: nur auf dem eigenen Rechner sein

Demonstration

3. Praxis

1. **Programm zum Verwalten von Schlüsseln**
   Gpg4win - GNU Privacy Guard for Windows
2. **E-Mail-Programm**
   Thunderbird
3. **Add-on, das die beiden verbindet**
   Enigmail

Verschlüsselungsprogramm
Verwaltung von Schlüsseln
Erzeugung von Schlüsseln

benutzt

Schreiben, Verschlüsseln,
Entschlüsseln,
Aufbewahren von Mails,
auch von mehreren Konten

Zuhause

1. Gpg4win installieren:
   http://www.gpg4win.de/
2. Thunderbird installieren:
   https://www.mozilla.org/de/thunderbird/
3. Enigmail installieren
   https://addons.mozilla.org/de/thunderbird/addon/enigmail/

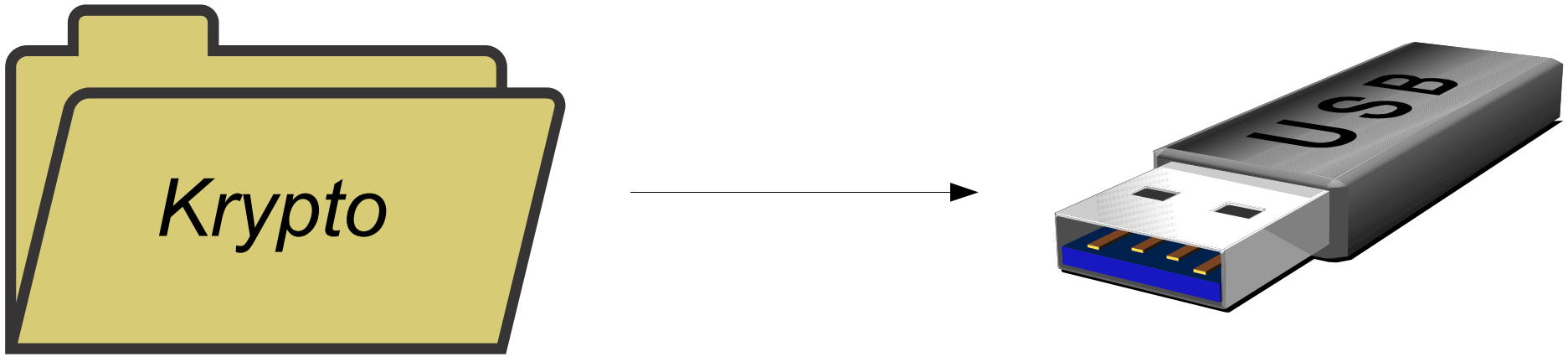
Schule

- bereits vorhanden: portabler Thunderbird, einschließlich Enigmail, einschließlich Gpg4win
- zu tun: Paket auf USB-Stick kopieren und von dort starten
- Kontodaten eingeben,
  Schlüssel erzeugen,
  Schlüssel austauschen

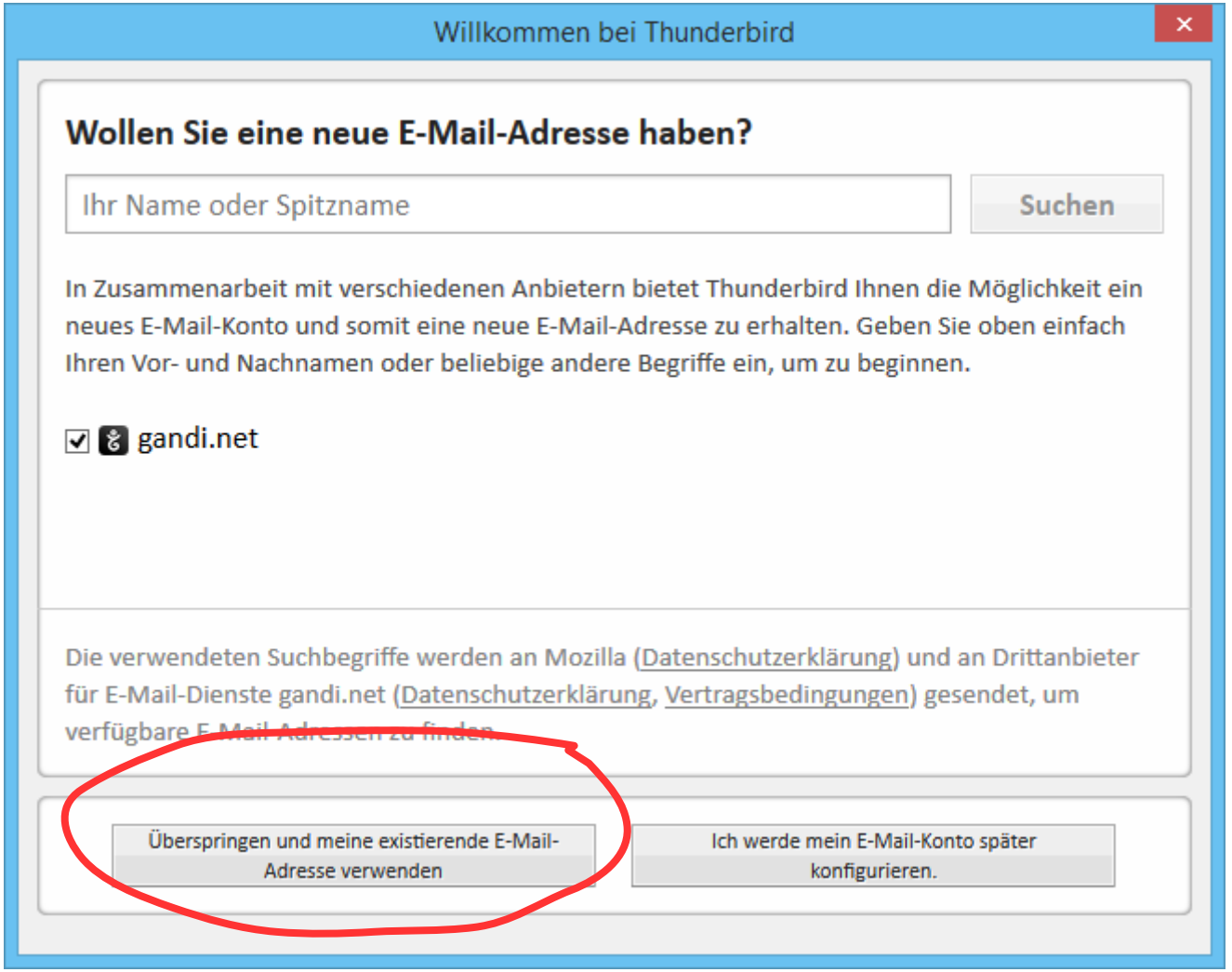
Schule

- bereits vorhanden: portabler Thunderbird, einschließlich Enigmail, einschließlich Gpg4win
- zu tun: Paket auf USB-Stick kopieren und von dort starten
- Kontodaten eingeben,
  Schlüssel erzeugen,
  Schlüssel austauschen

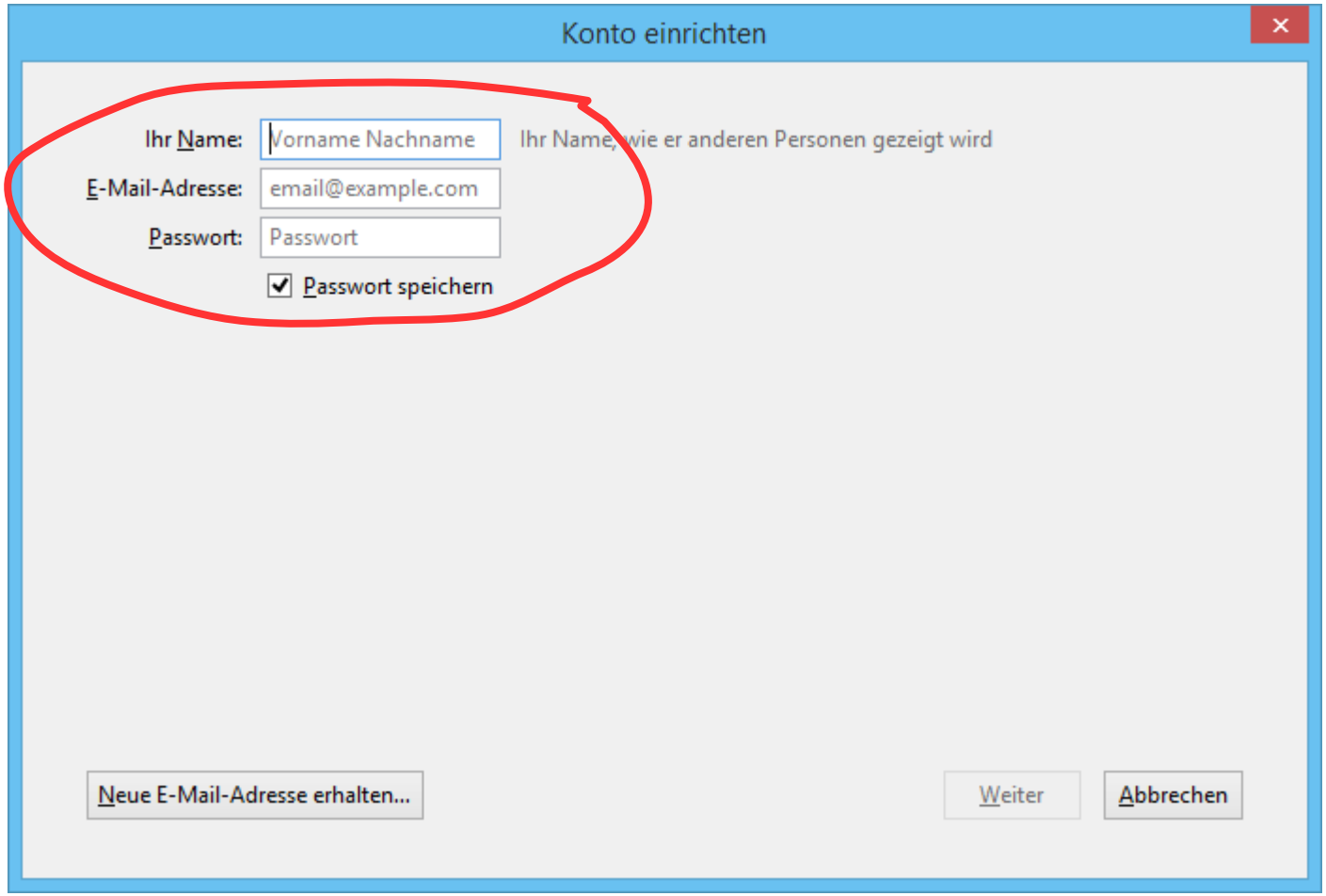
Anmelden, USB-Stick einstecken, Ordner "Krypto" kopieren



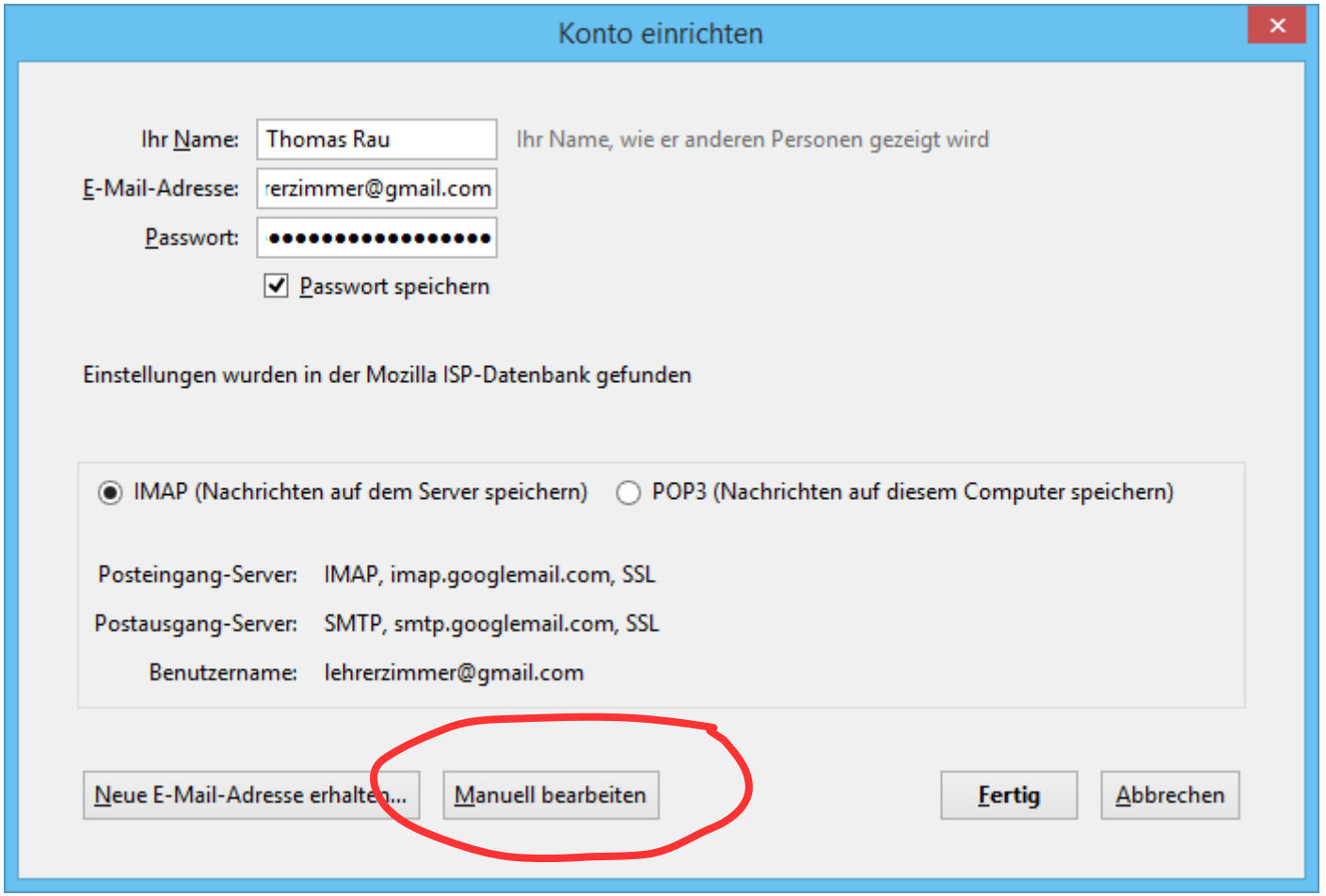
1. Starten: ThunderbirdPortable/ ThunderbirdPortable.exe



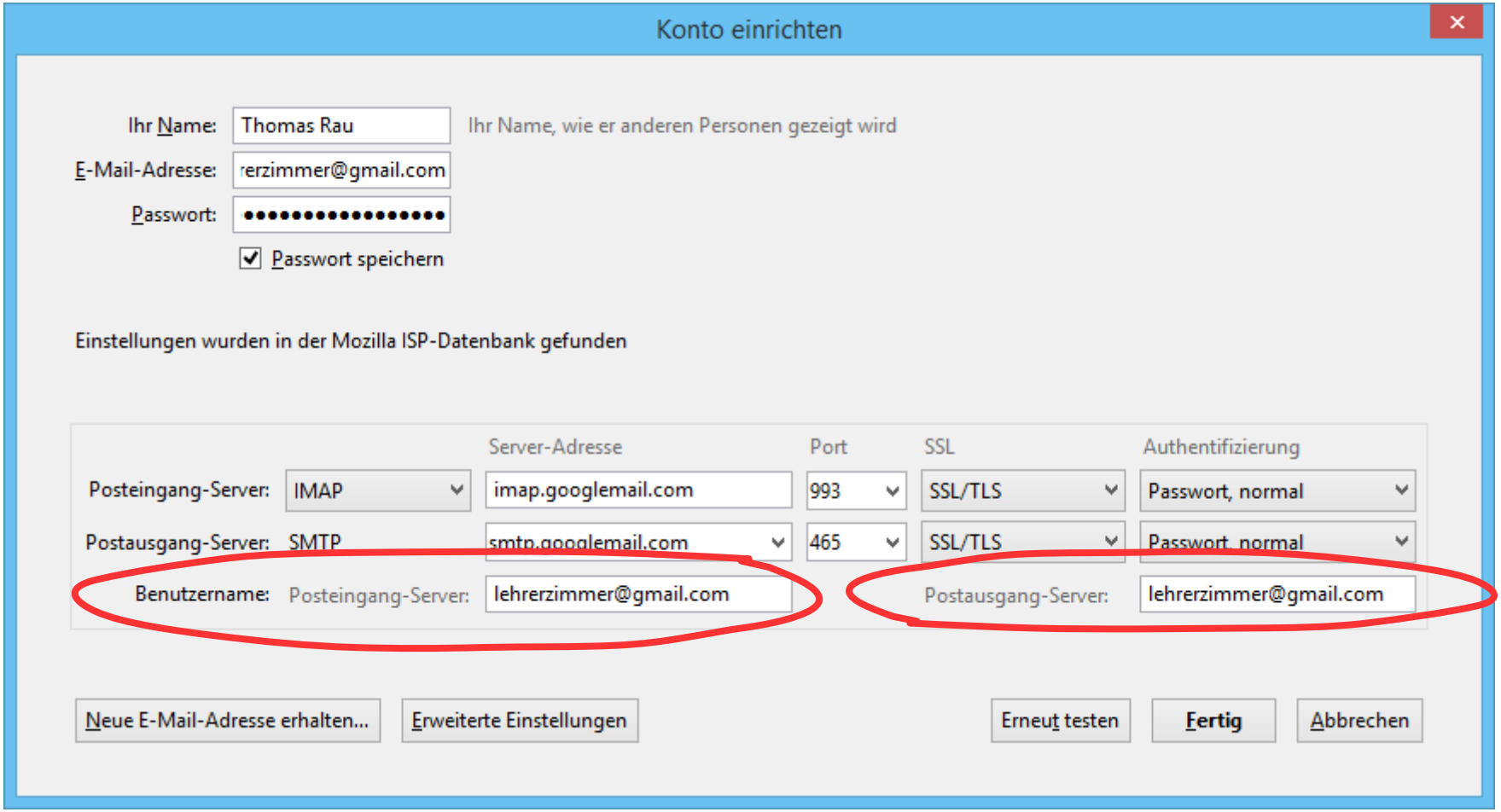
Eingabe einiger Daten (später folgend weitere)



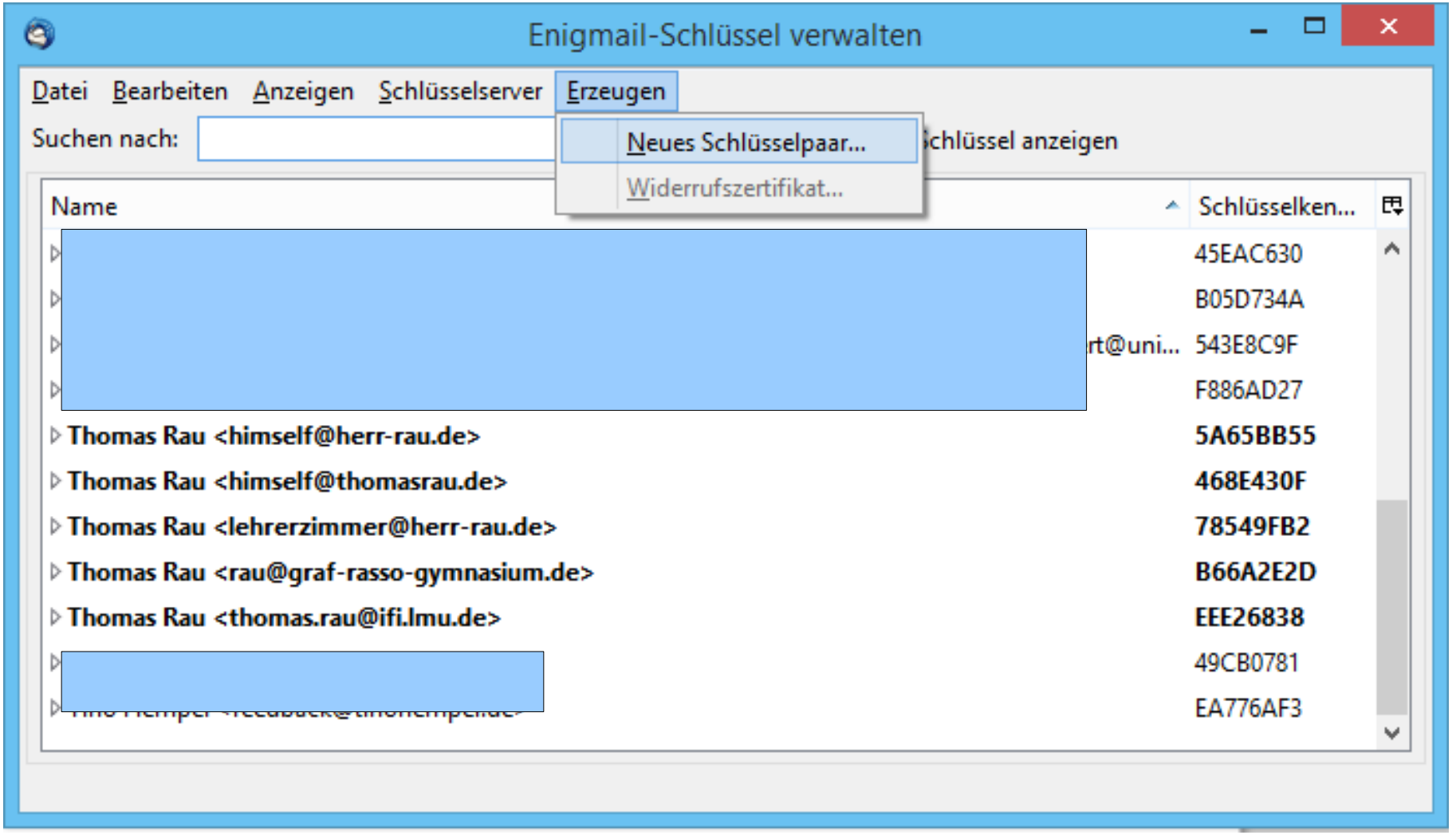
Thunderbird versucht, Server-Informationen zu ermitteln

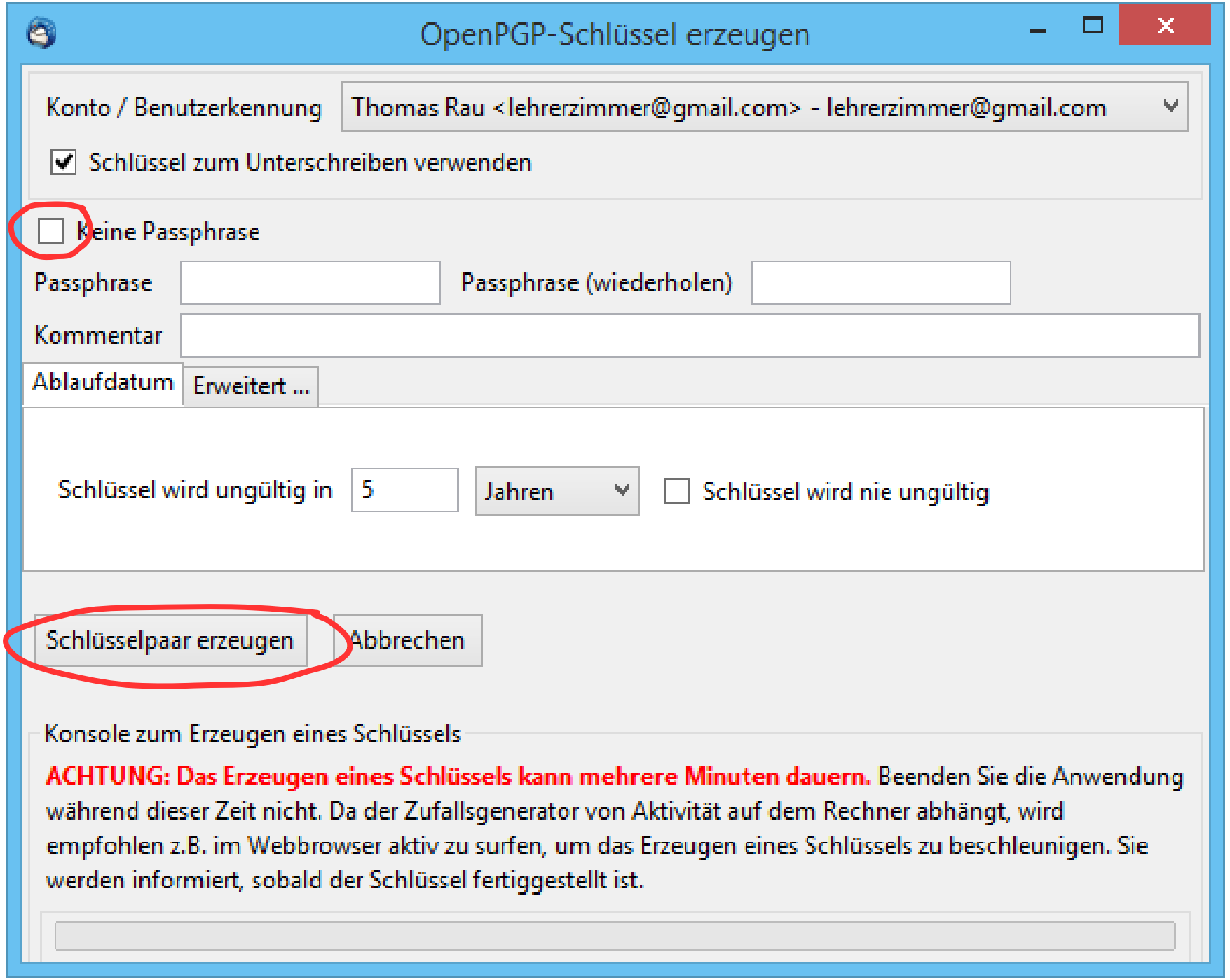


Manuelles Bearbeiten nötig (Benutzername)

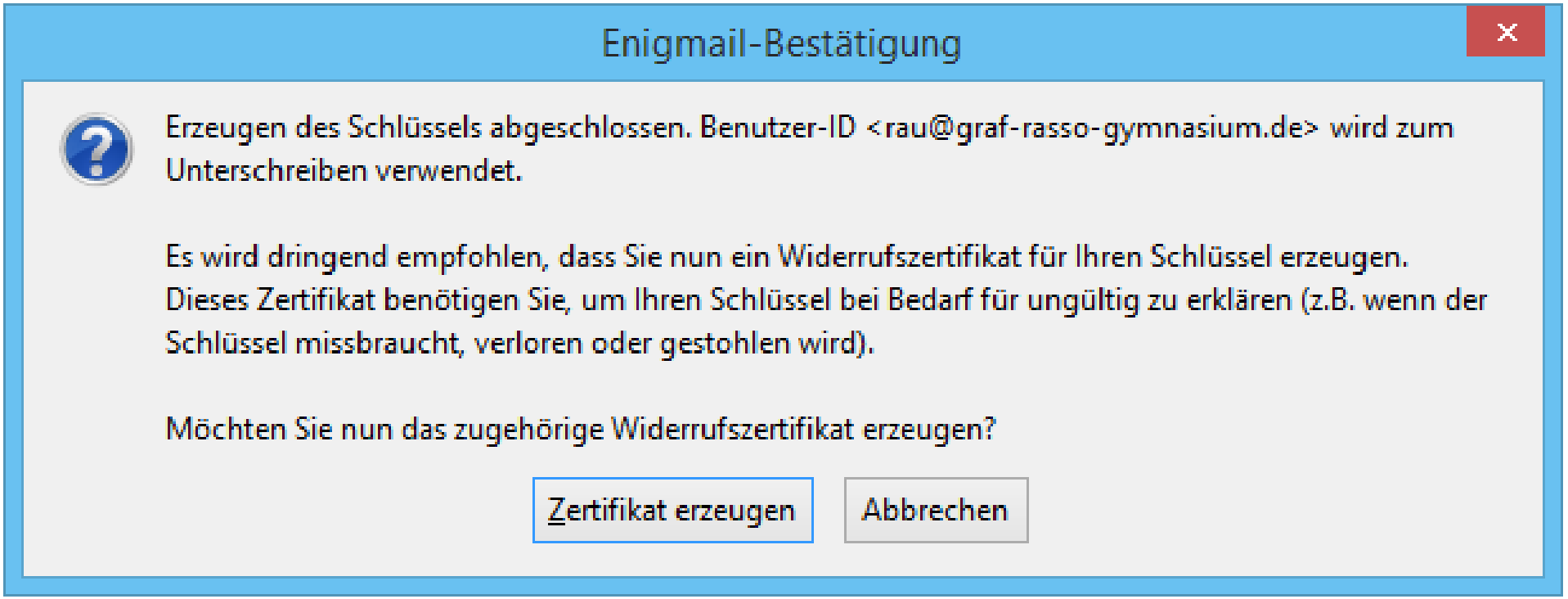


2. Anlegen der Schlüssel im Menü: Enigmail/Schlüssel verwalten...




OpenPGP-Schlüssel erzeugen
Konto / Benutzerkennung
Thomas Rau <lehrerzimmer@gmail.com> - lehrerzimmer@gmail.com
Schlüssel zum Unterschreiben verwenden
Keine Passphrase
Passphrase
Passphrase (wiederholen)
Kommentar
Ablaufdatum
Erweitert ...
Schlüssel wird ungültig in
5
Jahren
Schlüssel wird nie ungültig
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.

Widerrufszertifikat?



Veröffentlichen des public key (falls gewünscht)

- hochladen auf öffentlichen Server, z.B.
  pool.sks-keyservers.net
  keys.gnupg.net
- Anhängen des public key an eigene Mails
- Veröffentlichen auf Webseite

4. Weiterführendes

- Signieren statt Verschlüsseln
- Verwundbarkeit gegenüber Brute Force und anderen Angriffen: keine absolute Sicherheit
- In der Praxis (automatisch): Erst symmetrische Verschlüsselung mit einem gemeinsamen Schlüssel, nur der wird asymmetrisch verschlüsselt und mitgesendet
- Gewissheit: Woher weiß man, ob der öffentliche Schlüssel tatsächlich zu der Person gehört?
- Sicherheit durch Öffentlichkeit
- Sicherheit der Software
- Metadaten
- Verschlüsselung von Festplatten

4. Weiterführendes

- Schneller: Erst symmetrische Verschlüsselung mit einem gemeinsamen Schlüssel, nur der wird asymmetrisch verchlüsselt und mitgesendet
- Gewissheit: Woher weiß man, ob der öffentliche Schlüssel tatsächlich zu der Person gehört?
- Signieren zusätzlich zum Verschlüsseln
- Sicherheit durch Öffentlichkeit
- Ende-zu-Ende-Verschlüsselung (alternative: Schlüssel liegt beim Provider)
- Verwundbarkeit gegenüber Brute Force?
- Sicherheit der Software
- Metadaten

Nutzung unter Android

- Android:
  K-9 Mail (Mailprogramm)
  https://play.google.com/store/apps/details?id=com.fsck.k9&hl=de
- APG (Schlüsselverwaltung, arbeitet mit K-) zusammen)
  https://play.google.com/store/apps/details?id=org.thialfihar.android.apg&hl=de

Links

- Theorie zum Verschlüsselungsprinzip: http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/
- Ausprobieren im Browser mit Javascript: http://encrypt.alexanderjank.de/ http://www.hanewin.net/encrypt/PGcrypt.htm
- Öffentlicher Schlüssel von lehrerzimmer@herr-rau.de: http://www.herr-rau.de/wordpress/archiv/0x78549FB2.asc