Cryptoschnack - Mail

Photo: kekko, CC BY-ND 2.0-Lizenz

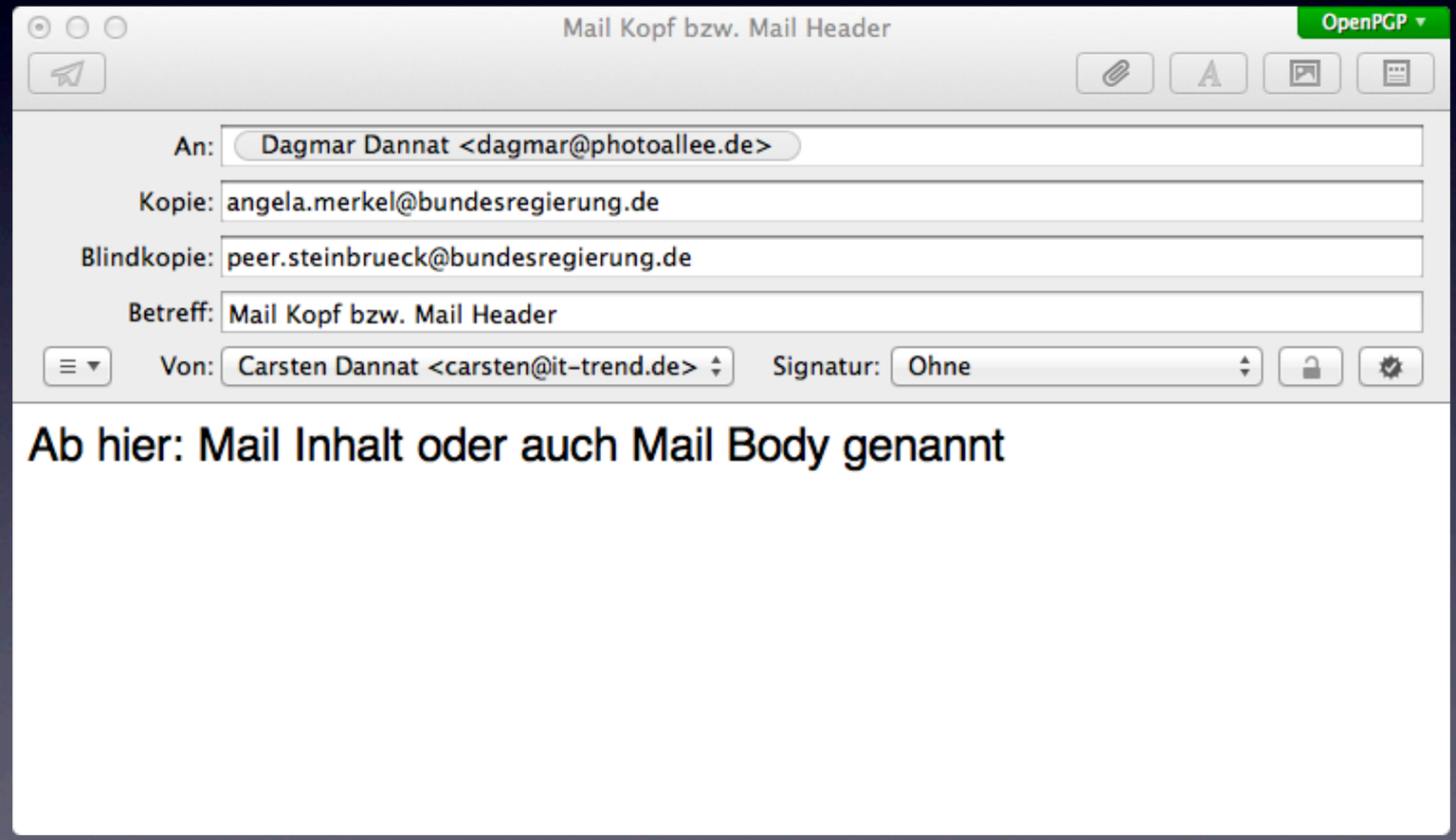
V I.I

Inhalt

- Einleitung
- Passwörter
- Cryptoverfahren
- Mailverschlüsselung
- Fragen und Antworten

Einleitung

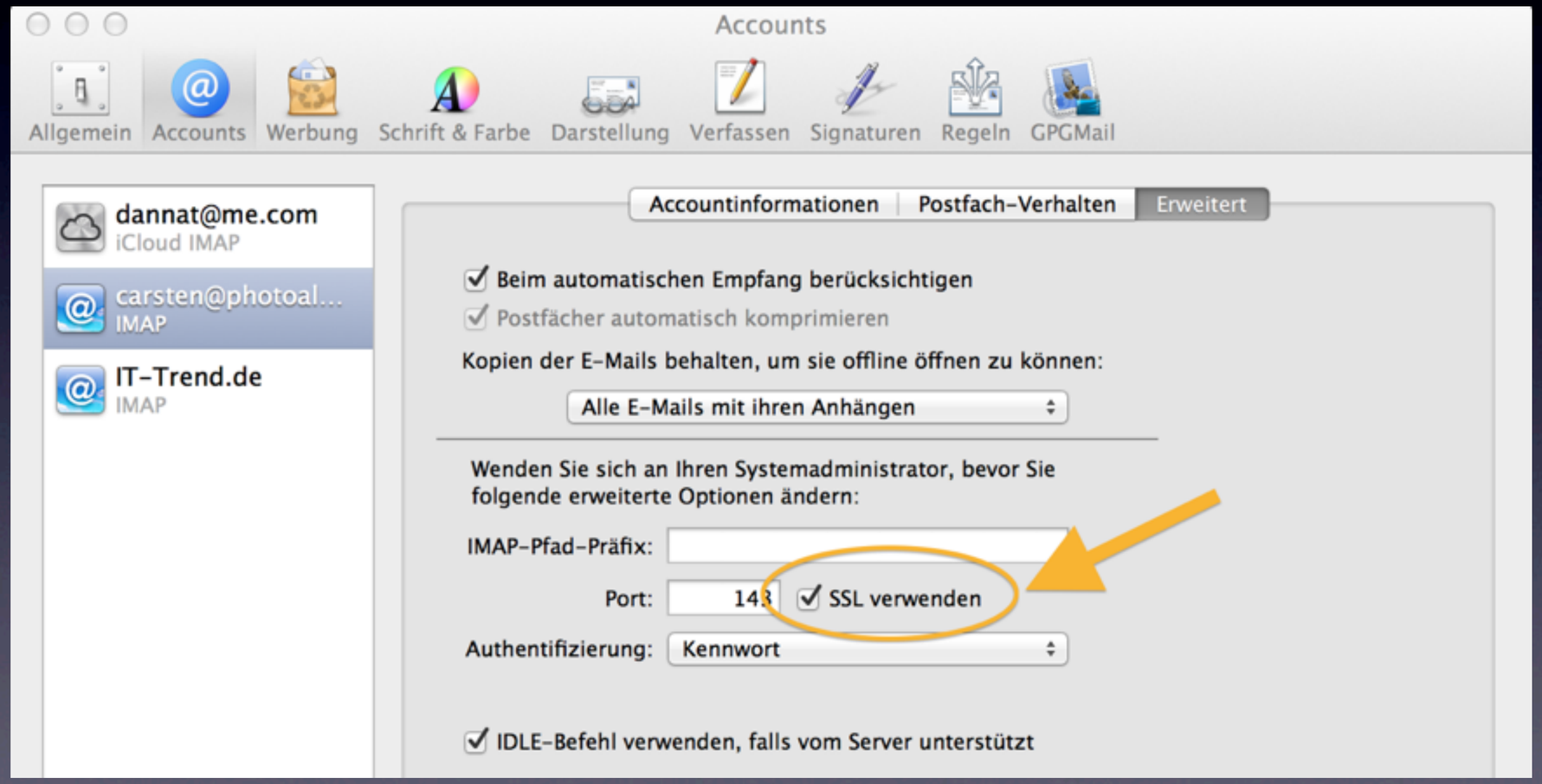
eMails sind Postkarten!



eMail
Made in Germany

Verschlüsselung beim Transport der eMail untereinander.
eMail liegt aber weiterhin unverschlüsselt auf dem Server des Anbieters.

Einleitung


Accounts
Allgemein
Accounts
Werbung
Schrift & Farbe
Darstellung
Verfassen
Signaturen
Regeln
GPGMail
dannat@me.com
iCloud IMAP
carsten@photoal...
IMAP
IT-Trend.de
IMAP
Accountinformationen
Postfach-Verhalten
Erweitert
Beim automatischen Empfang berücksichtigen
Postfächer automatisch komprimieren
Kopien der E-Mails behalten, um sie offline öffnen zu können:
Alle E-Mails mit ihren Anhängen
Wenden Sie sich an Ihren Systemadministrator, bevor Sie folgende erweiterte Optionen ändern:
IMAP-Pfad-Präfix:
Port:
143
SSL verwenden
Authentifizierung:
Kennwort
IDLE-Befehl verwenden, falls vom Server unterstützt

Einleitung

Sicherheit bedeutet Komfortverlust.

Photo: niiicedave CC BY-SA 2.0

Der Empfänger einer eMail muss ermöglichen, daß der Inhalt nur auf seinem Rechner und dem Rechner des Absenders im Klartext lesbar ist.

Passwörter

geheim

1965

angela

asdfghjk

NePmm10ZiegP!

Nur ein Passwort mit mindestens 10 Zeichen
ist ein gutes Passwort!

A-Z + a-z (52 Zeichen)

- 6 Zeichen: 20 Sekunden
- 10 Zeichen: 31.536.000 Sekunden = 5 Jahre

Quelle: Wikipedia

A-Z + a-z + Sonderzeichen
(96 Zeichen)

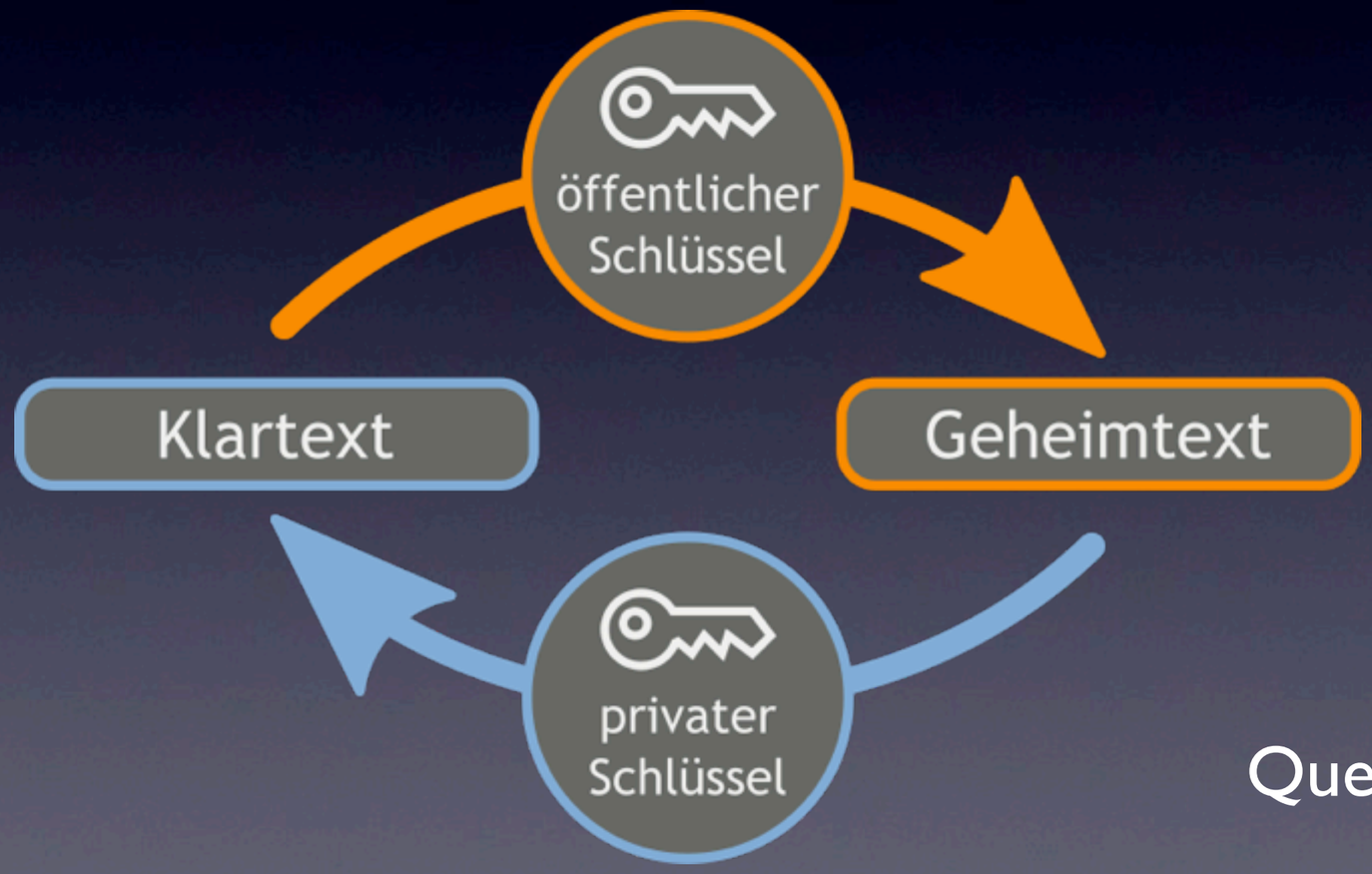
- 6 Zeichen: 13 Minuten
- 10 Zeichen: 2108 Jahre

Quelle: Wikipedia

Public Key Cryptoverfahren

- GnuPG (GNU Privacy Guard, RFC 4880)
- PGP - Ein Public-Key-Verschlüsselungsverfahren
- Öffentlicher Schlüssel zum Verschlüsseln
- Geheimer Schlüssel zum Entschlüsseln

Asymmetrische Verschlüsselung



Quelle: Wikipedia

Öffentliche Schlüssel

- per eMail Anhang PGP/MIME
- als Datei importieren
- Keyserver
- Demo - Keyserver

Mailverschlüsselung

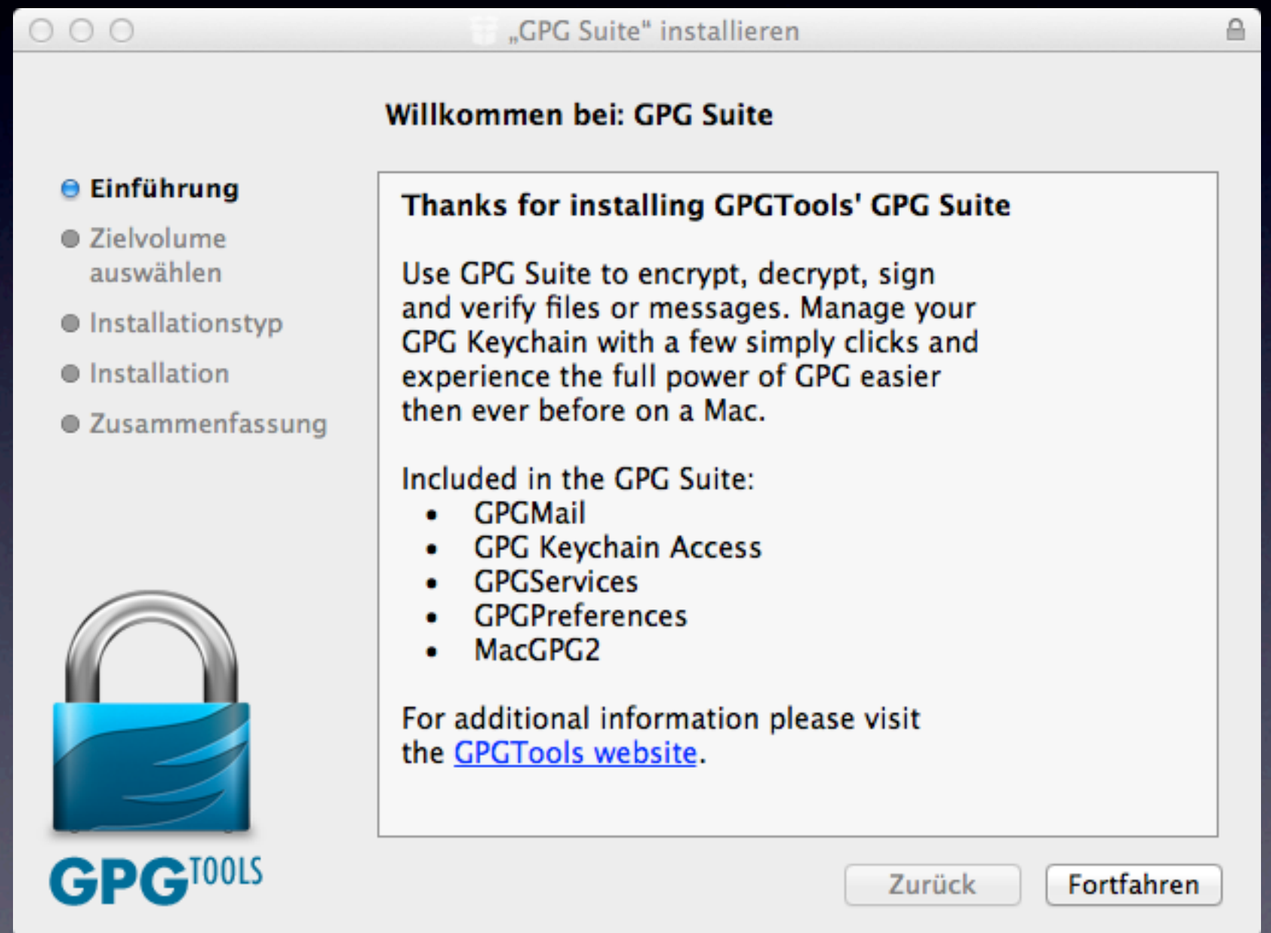
Wir benötigen:

GPGTools
http://gpgtools.org

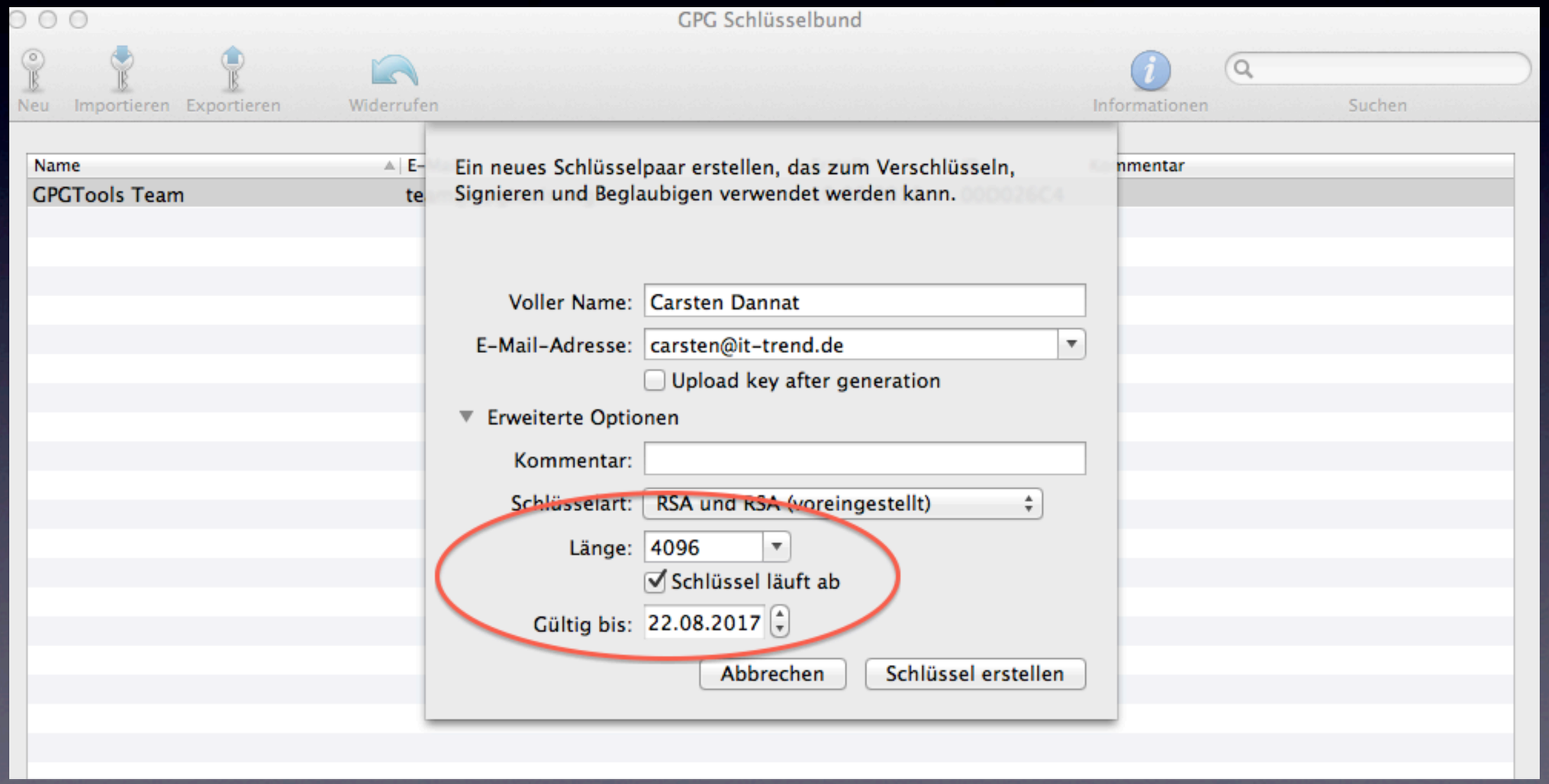
OS X 10.6 oder höher

Installation GPGTools

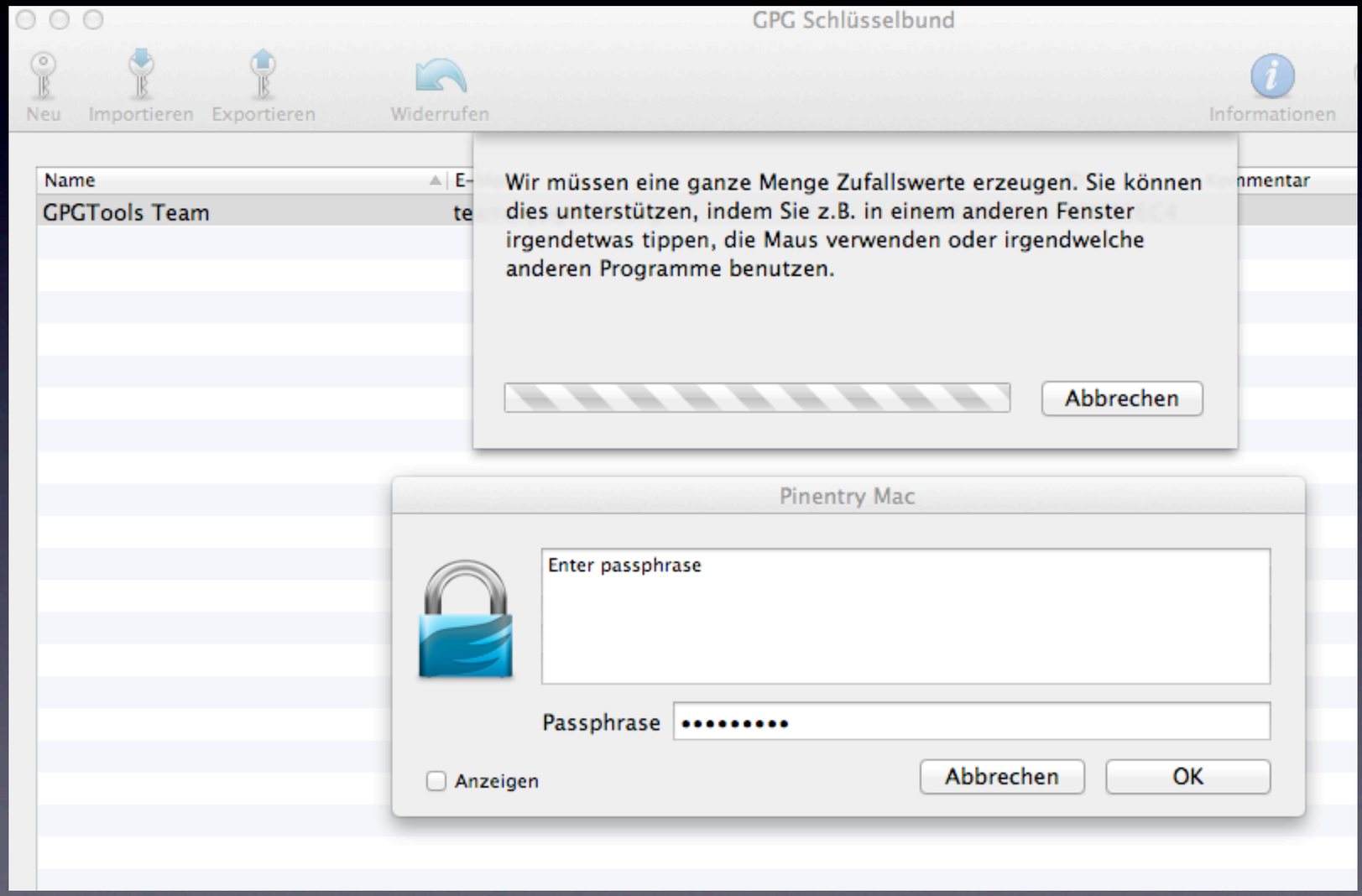
Installation GPGTools



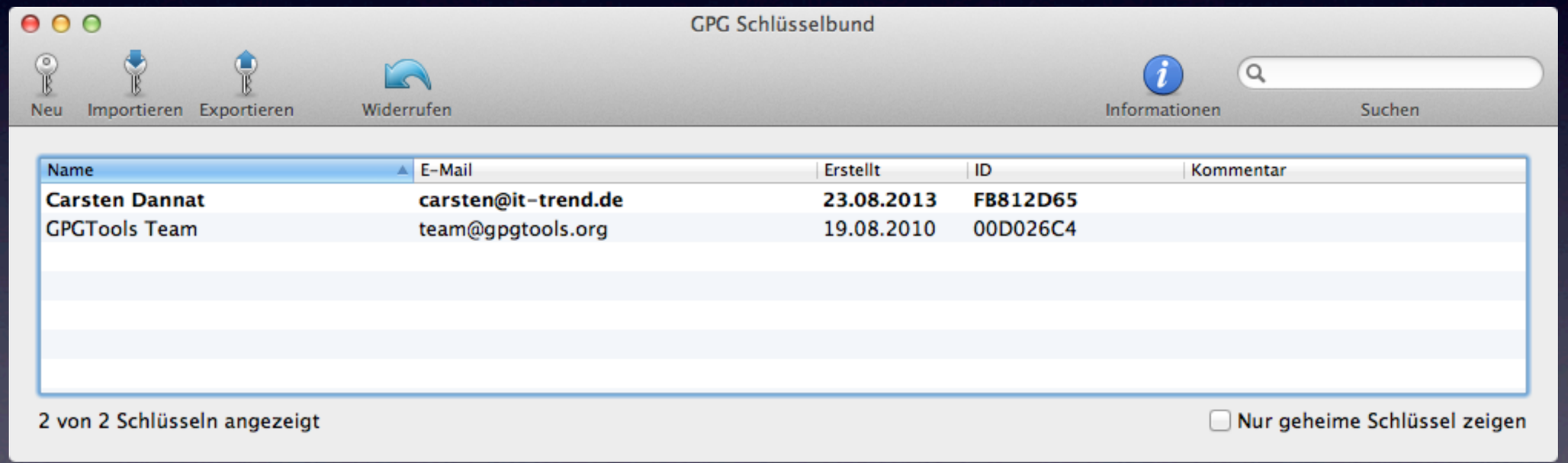
Installation GPGTools



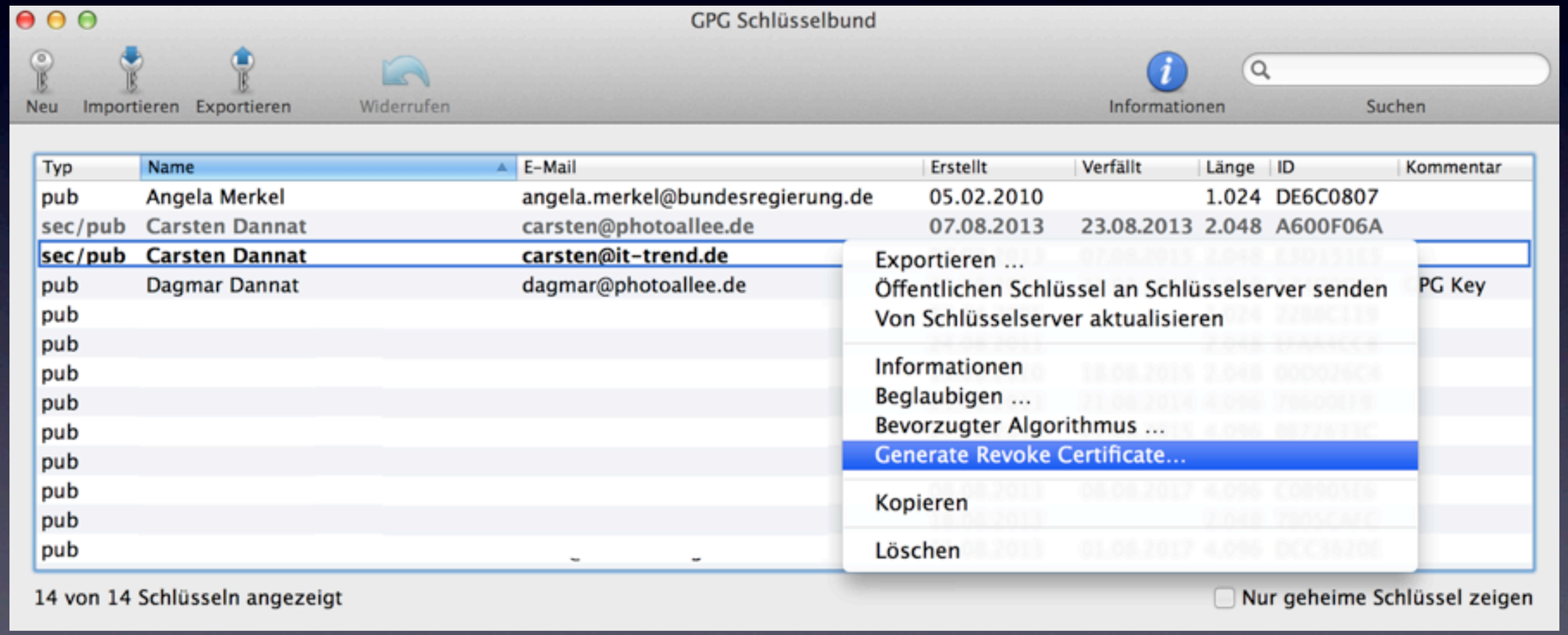
Installation GPGTools



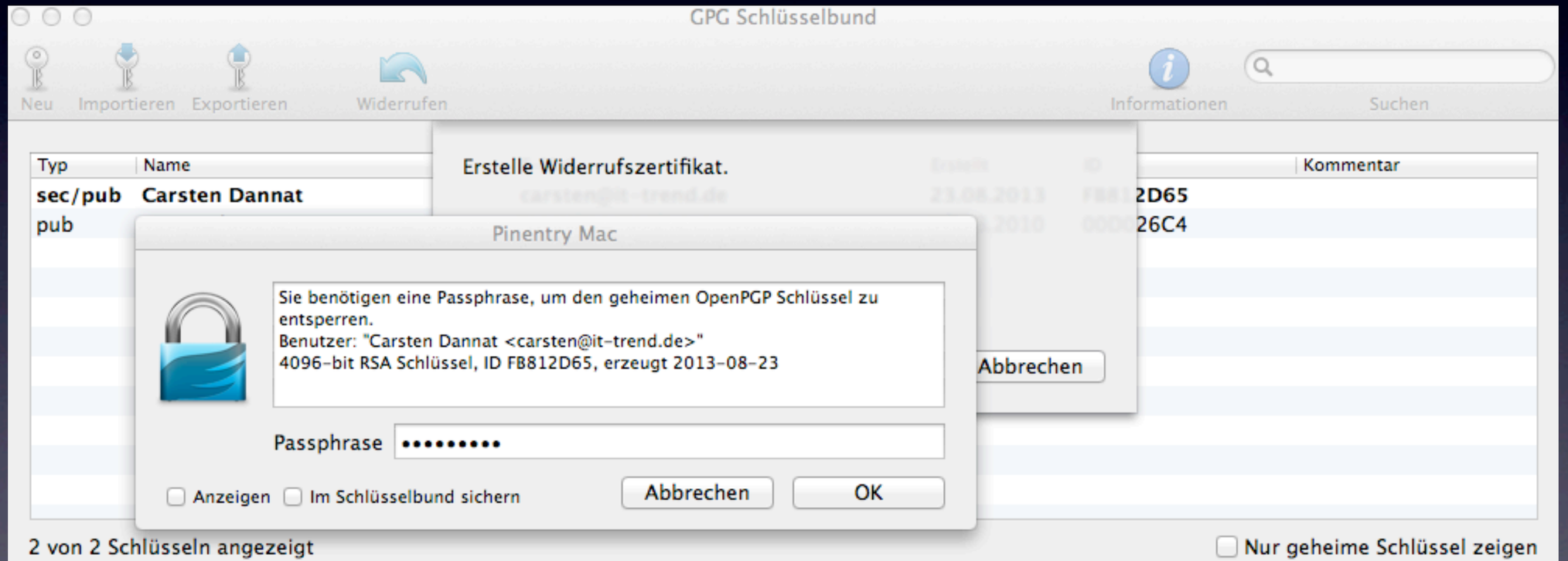
Installation GPGTools



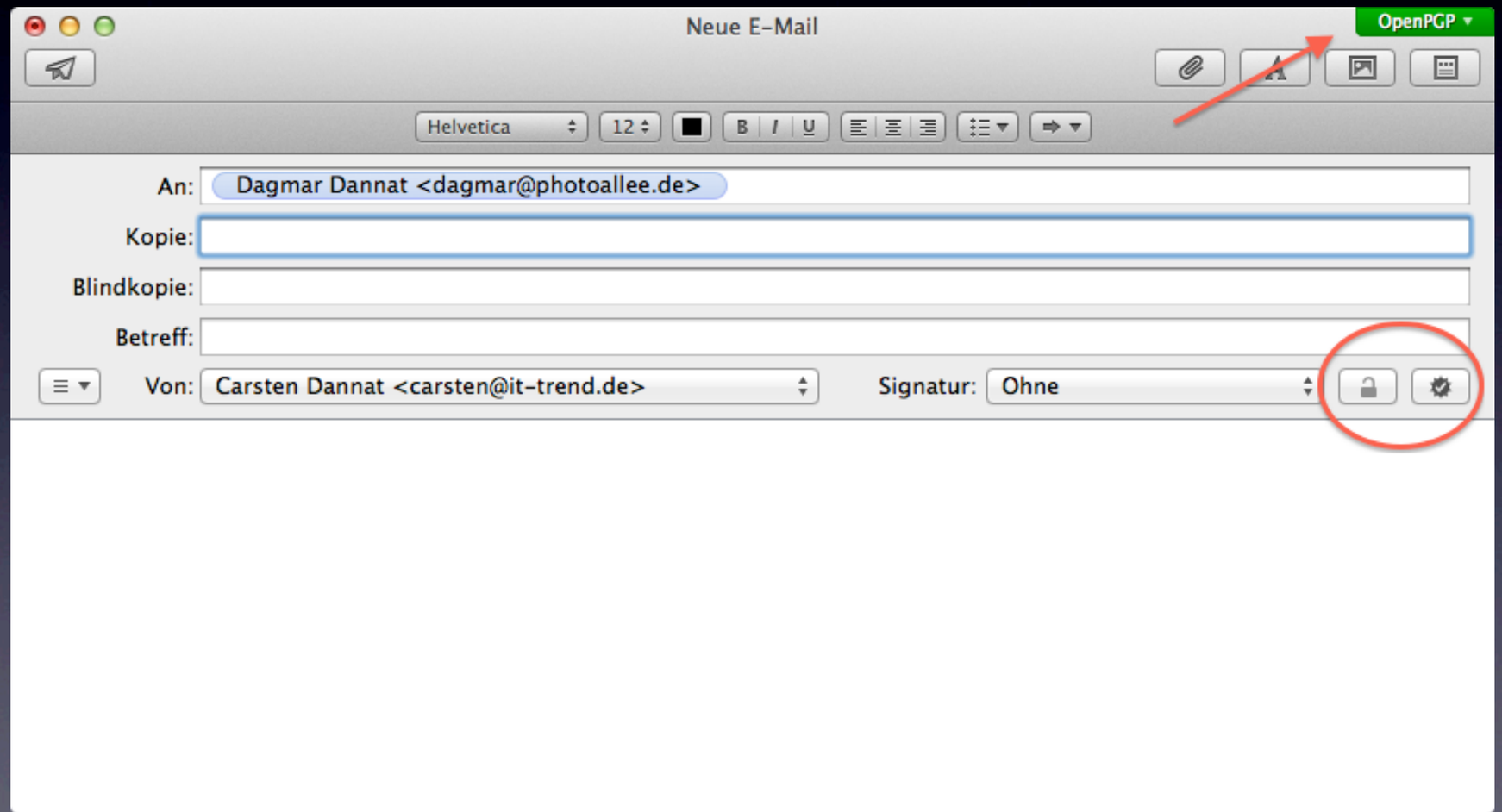
Installation GPGTools



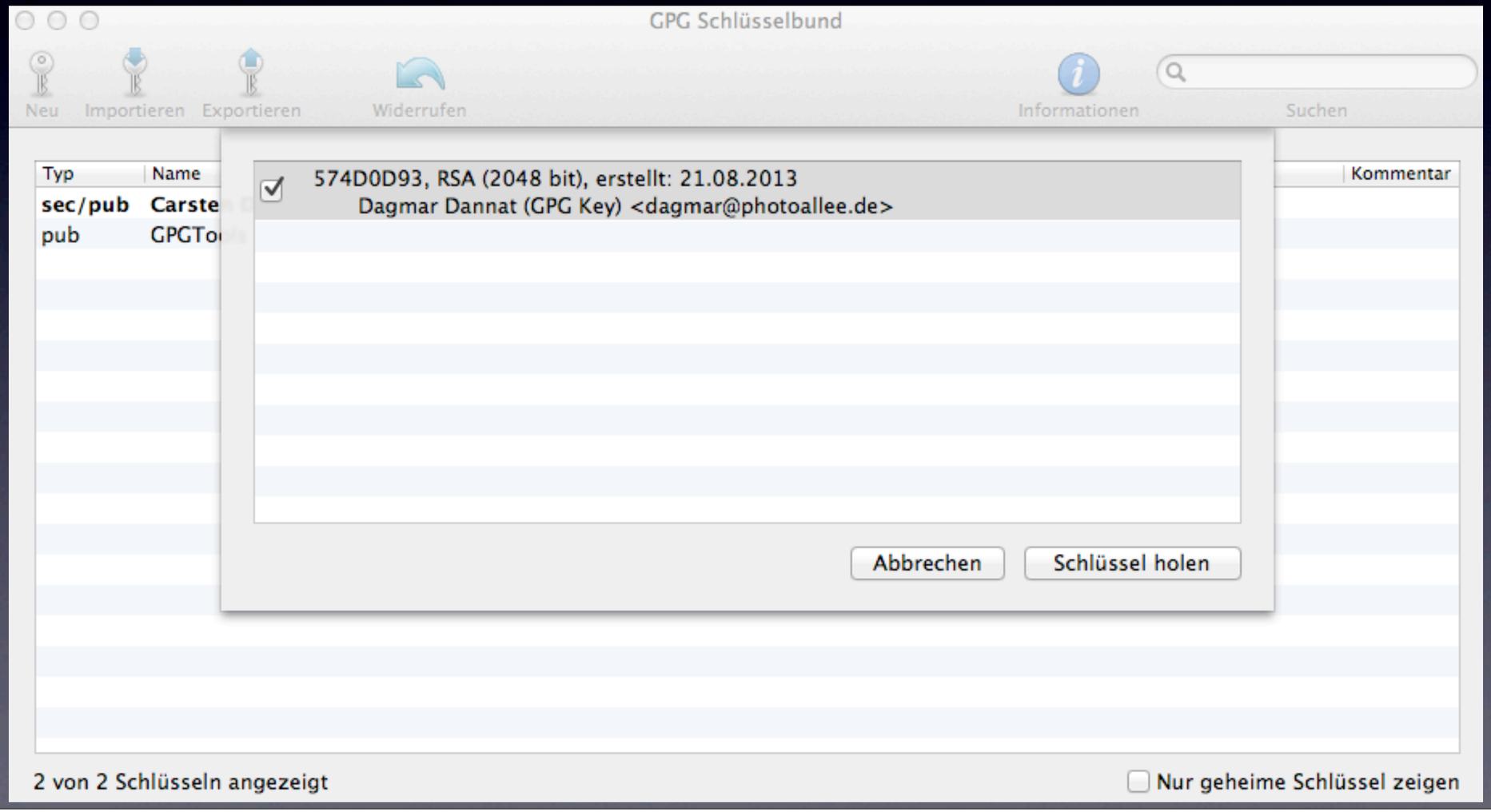
Installation GPGTools



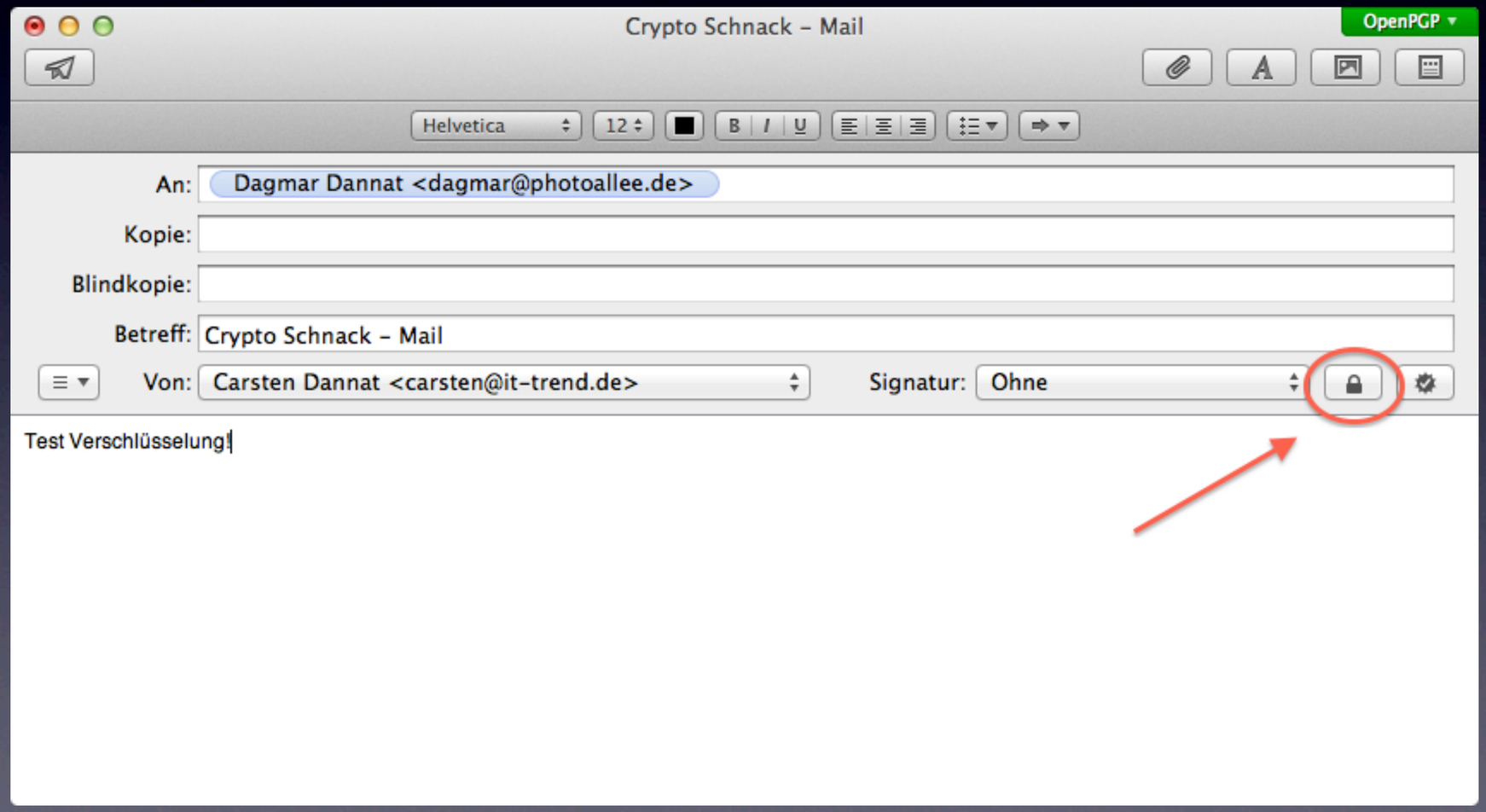
Installation GPGTools



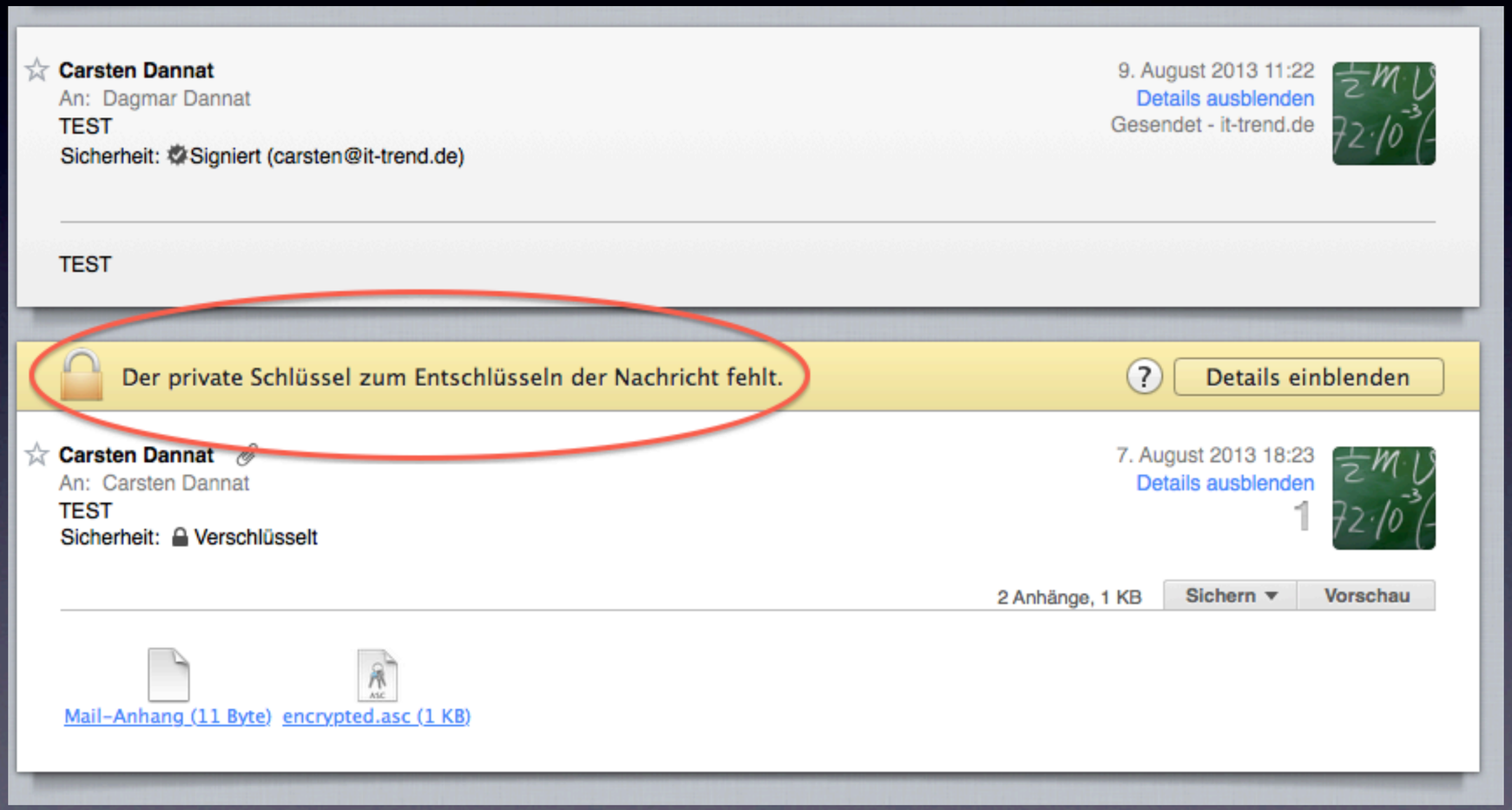
Installation GPGTools



Installation GPGTools



Installation GPGTools



Fragen und Antworten

- Wie kann ich überprüfen, ob der öffentliche Schlüssel zu Angela Merkel gehört?
- Web of Trust
- Keyserver Probleme (Spam, Ewiges Gedächtnis, Verbindungen, ...)
- ...

Herzlichen Dank

eMail: carsten@it-trend.de

twitter: @carstendannat

August 2013