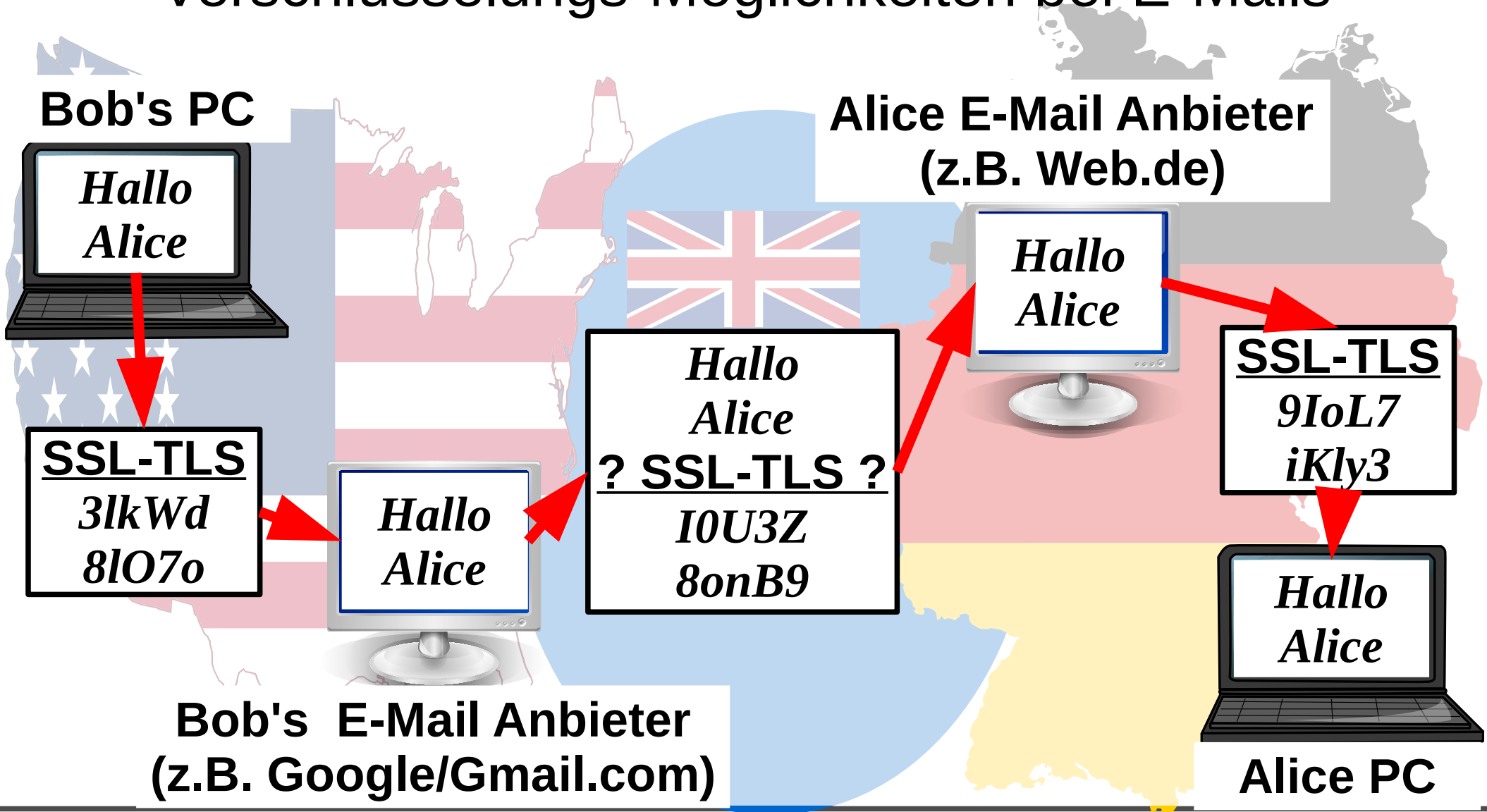
CryptoParty

BÜNDNIS 90
DIE GRÜNEN

E-Mail Verschlüsselung mit PGP/GnuPG

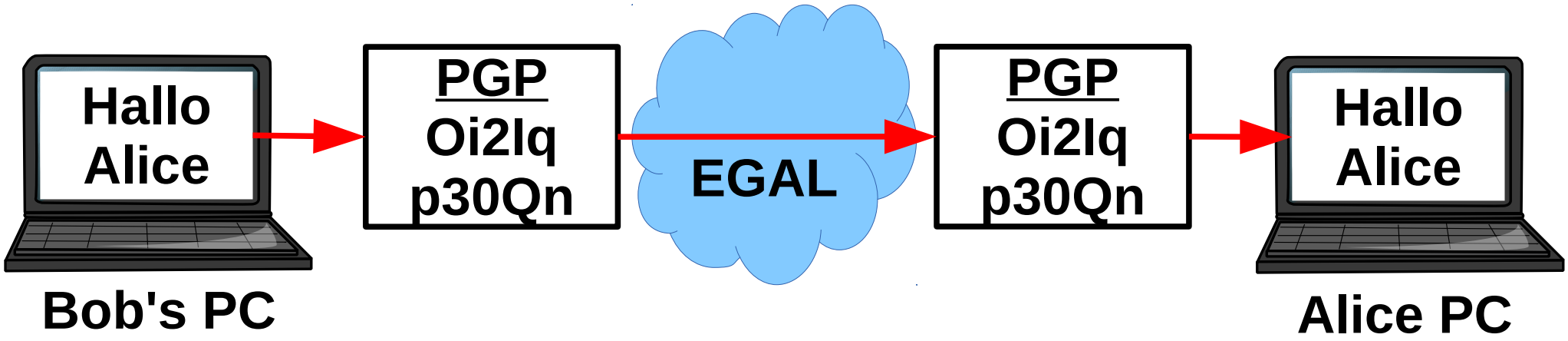
CryptoParty

„klassische“ unzureichende Verschlüsselungs-Möglichkeiten bei E-Mails



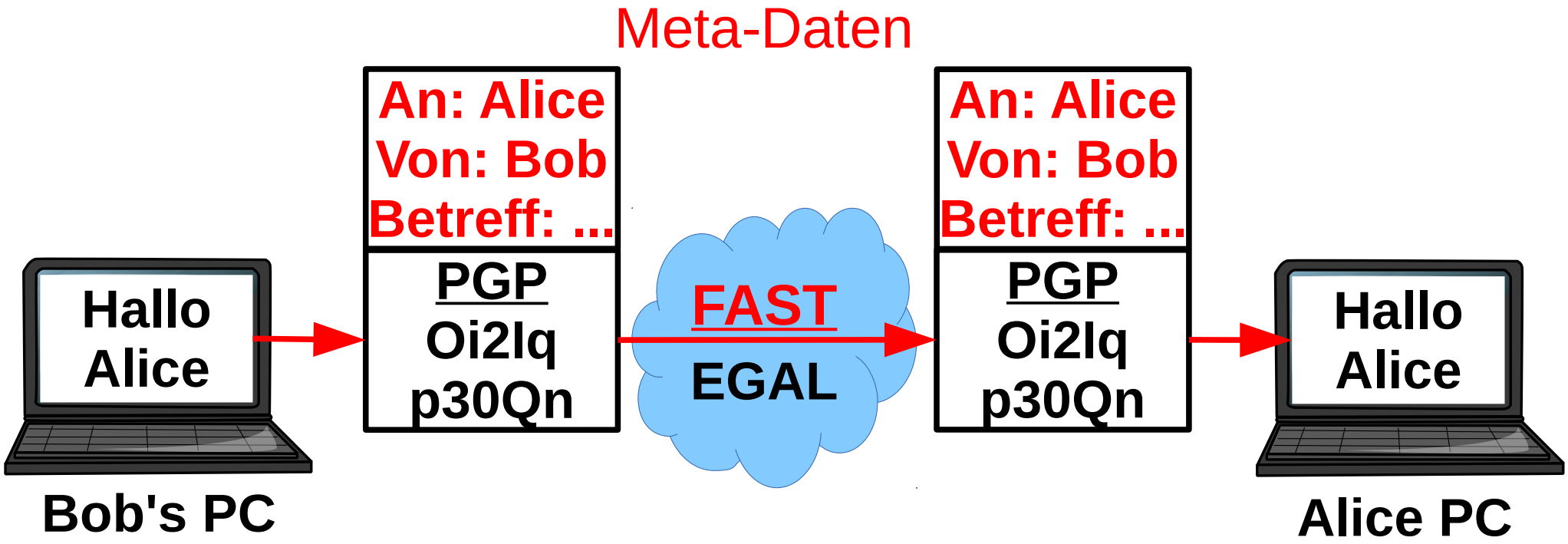
CryptoParty

Ende-zu-Ende Verschlüsselung



CryptoParty

Ende-zu-Ende Verschlüsselung



CryptoParty

3 Programme

Thunderbird – E-Mail-Programm (ähnlich Outlook)

GnuPG – verschlüsselt die E-Mails mit PGP

Enigmail – verbindet Thunderbird und GnuPG

CryptoParty

3 Programme

Alle Links auf: **http://kolahilft.de/cryptoparty**

In dieser Reihenfolge installieren:

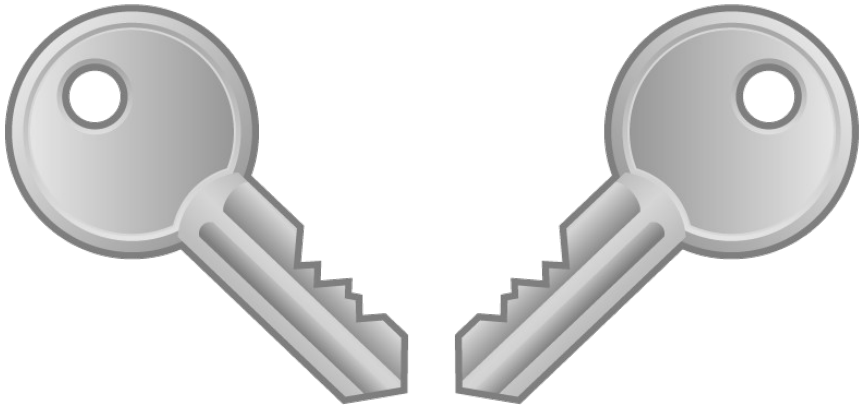
1. Thunderbird

2. GnuPG

3. Enigmail
   In Thunderbird:
   Add-ons => Suchen (oben rechts) => Enigmail

CryptoParty

Öffentlicher und Privater Schlüssel
Public Key / Private Key



Zwei Anwendungszwecke:
Verschlüsseln
Signieren

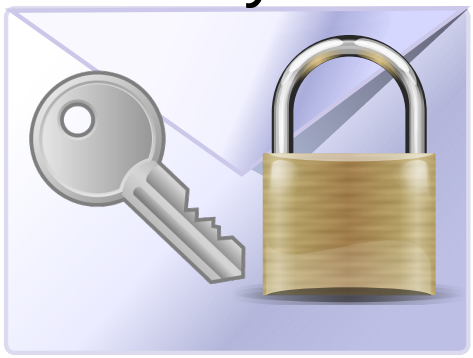
CryptoParty

Verschlüsseln

Alice (Absender)
Public Key von Bob

nur zum Verschließen

Bob (Empfänger)
Private Key von Bob



zum Öffnen

Jeder kann Verschlüsseln
Nur der Empfänger kann Entschlüsseln

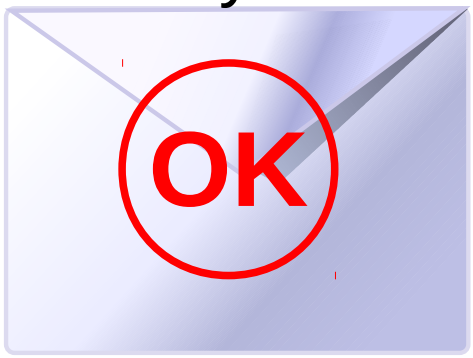
CryptoParty

Signieren

Alice (Absender)
Private Key von Alice

zum Signieren

Bob (Empfänger)
Public Key von Alice



nur zum Signatur Prüfen

Nur der Absender kann als er selbst signieren
Jeder kann die Signatur prüfen

CryptoParty

Unterschied:

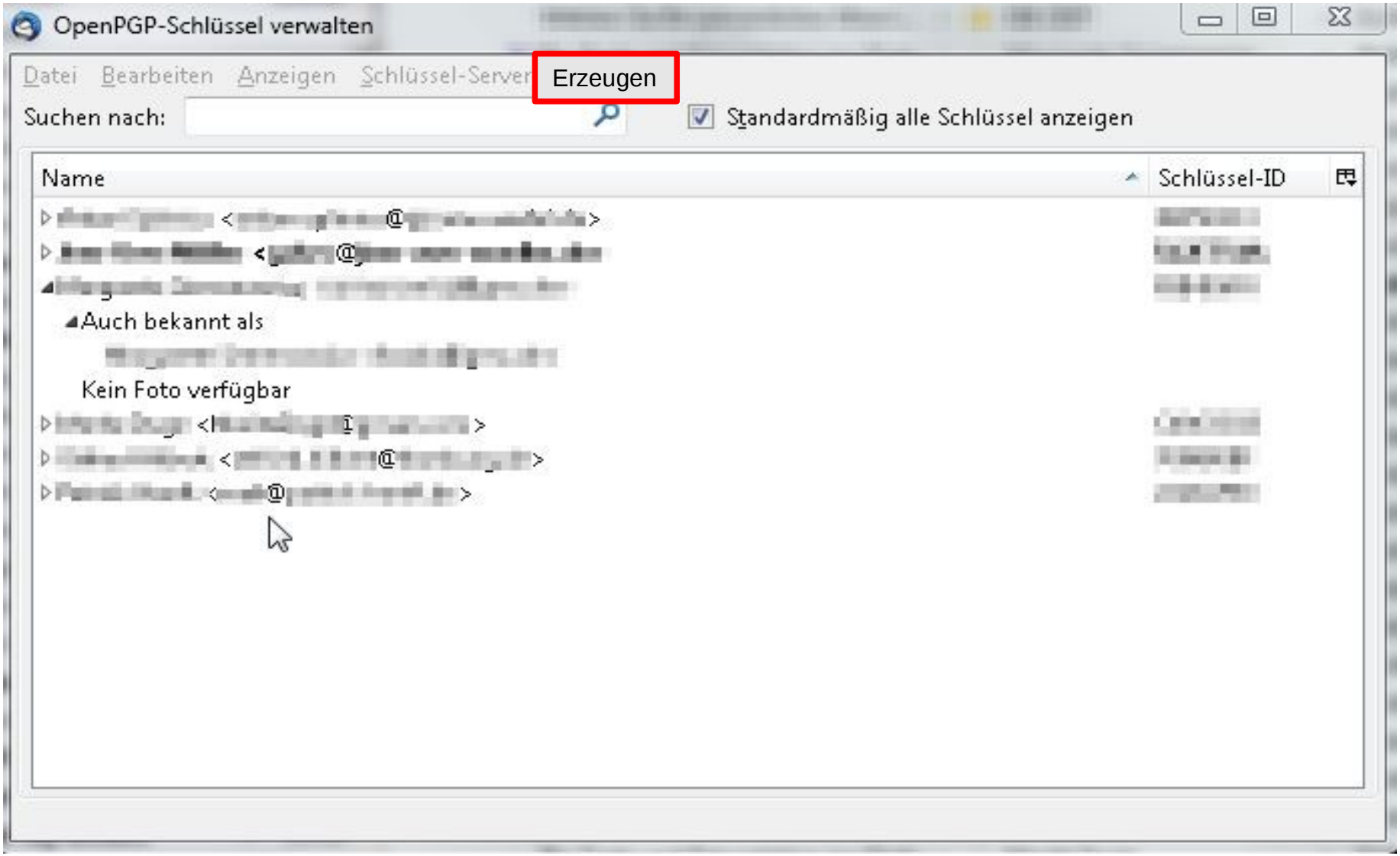
Verschlüsseln	**Signieren**
kein Fremder kann mitlesen	Authentizität
Schutz vor Überwachung	echt / nicht verändert
	ggf. Beweismittel
Mailinglisten: kompliziert	Mailinglisten: einfach

kann jeweils einzeln oder kombiniert verwendet werden

CryptoParty

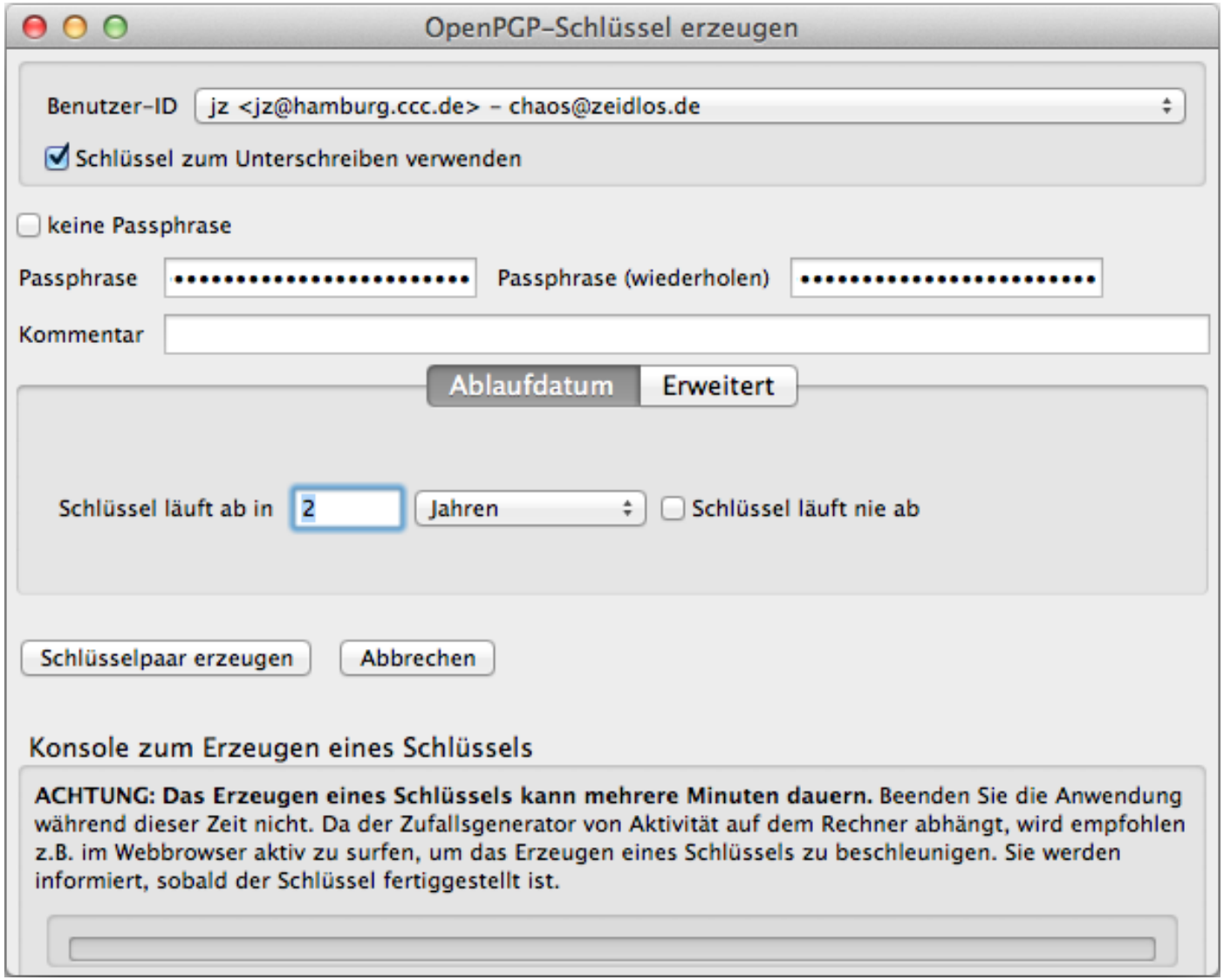
BÜNDNIS 90
DIE GRÜNEN

Enigmail



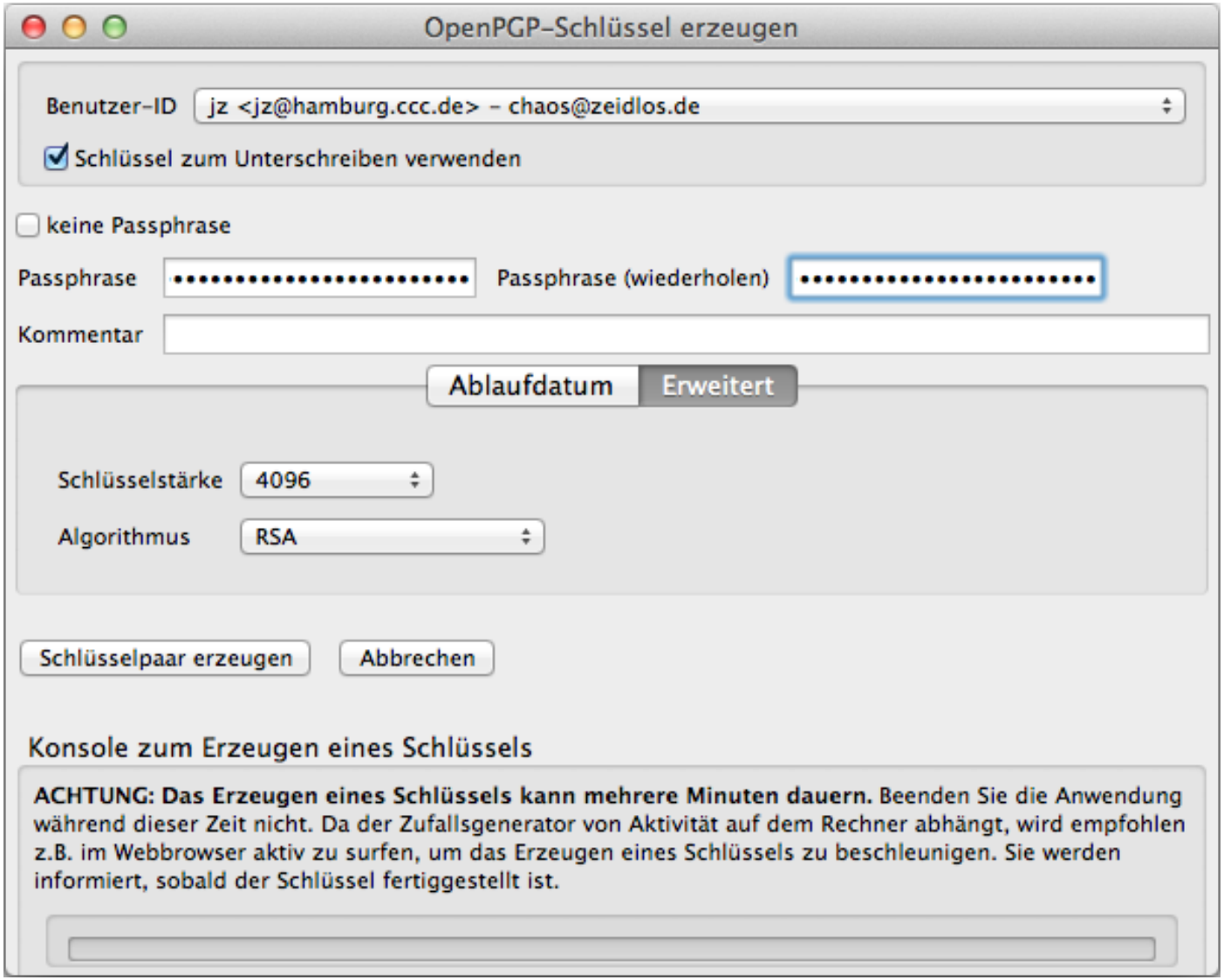
CryptoParty

Enigmail



CryptoParty

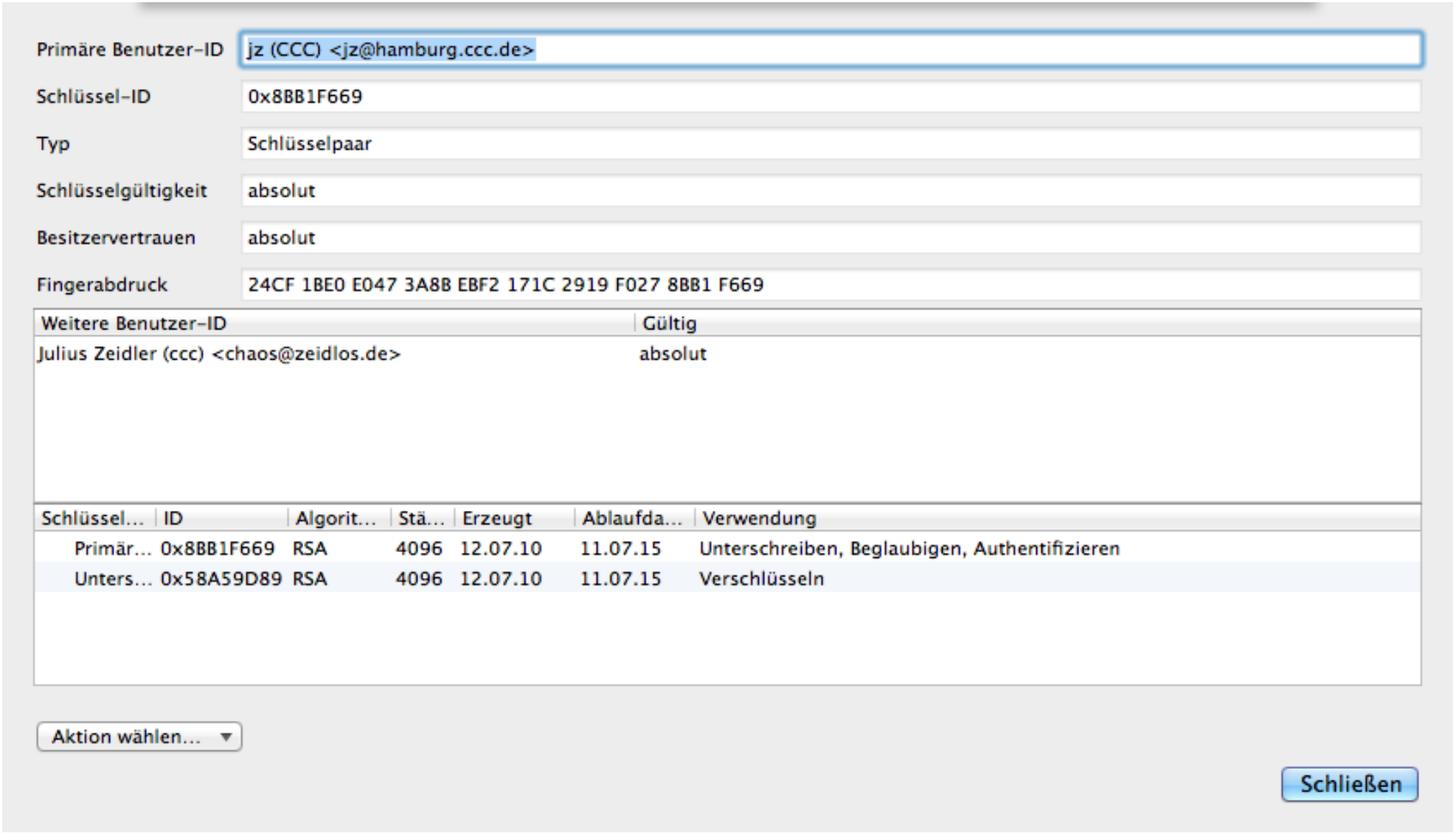
Enigmail



CryptoParty

BÜNDNIS 90
DIE GRÜNEN

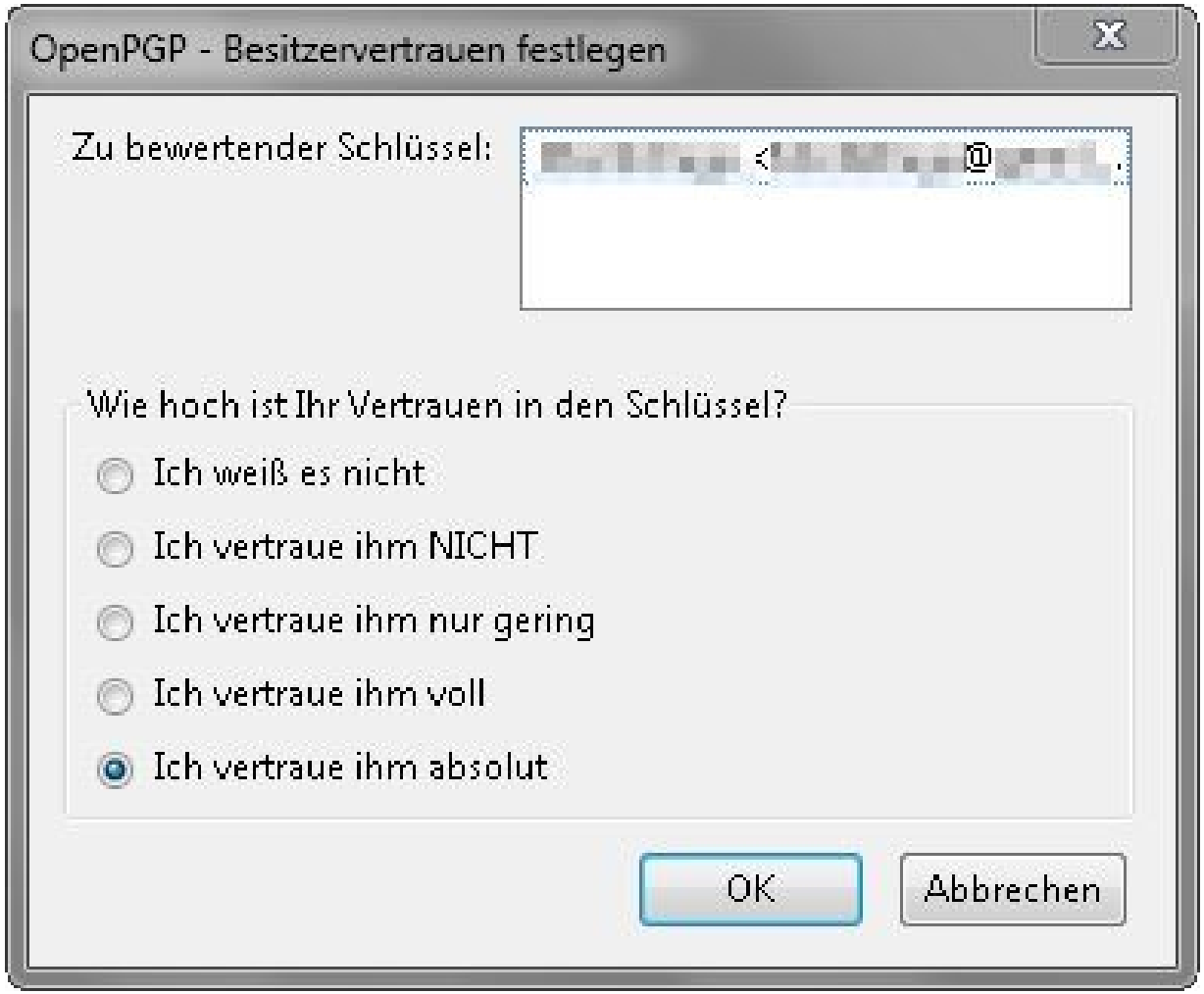
Enigmail



CryptoParty

BÜNDNIS 90
DIE GRÜNEN

Vertrauensstufen für fremde Schlüssel in Enigmail



CryptoParty

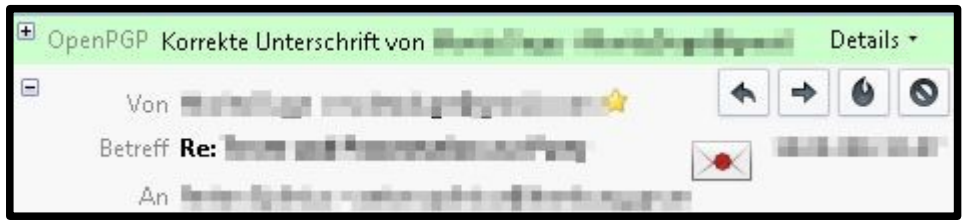
BÜNDNIS 90
DIE GRÜNEN

Vertrauensstufen für fremde Schlüssel in Enigmail

Keine Entschlüsselung

Entschlüsselt, aber Unterschrift nicht geprüft, das Public Key nicht im Besitz

Authentizität bestätigt, aber Du hast nicht selbst die Vertrauensstufe definiert



Absolutes Vertrauen

CryptoParty

Keyserver und Problematik des sozialen Graphen durch signierte Schlüssel

- A signiert B
- B signiert C und D
- D signiert A und B

N braucht nur Zugriff zum öffentlichen Keyserver, um sich ein Kommunikationsnetzwerk abzuleiten.

Besser:
- Schlüssel per E-Mail austauschen.

Am sichersten:
- Schlüssel direkt ohne Netz austauschen.

CryptoParty

Quellen

Abbildungen von:

https://openclipart.org

https://commons.wikimedia.org

CryptoParty

Folien-Lizenz

Autoren: Moritz Duge, Jens-Uwe Möller, Patrick Hanft,
Otfried Hilbert