

www.kolahilft.de/cryptoparty

WLAN: BETAHAUS

KEY: betahaus10?

CryptoParty

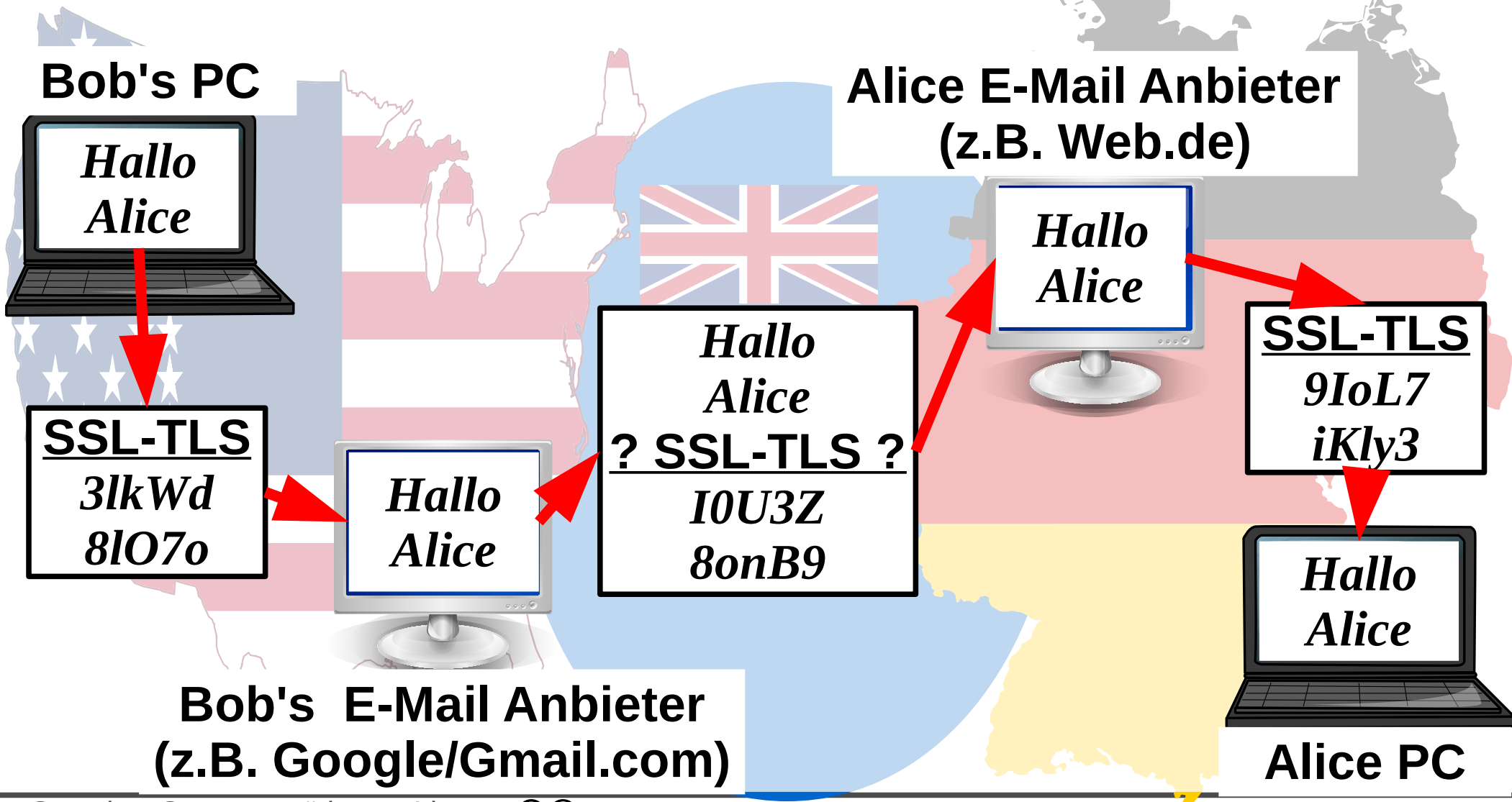


E-Mail Verschlüsselung mit PGP/GnuPG



CryptoParty

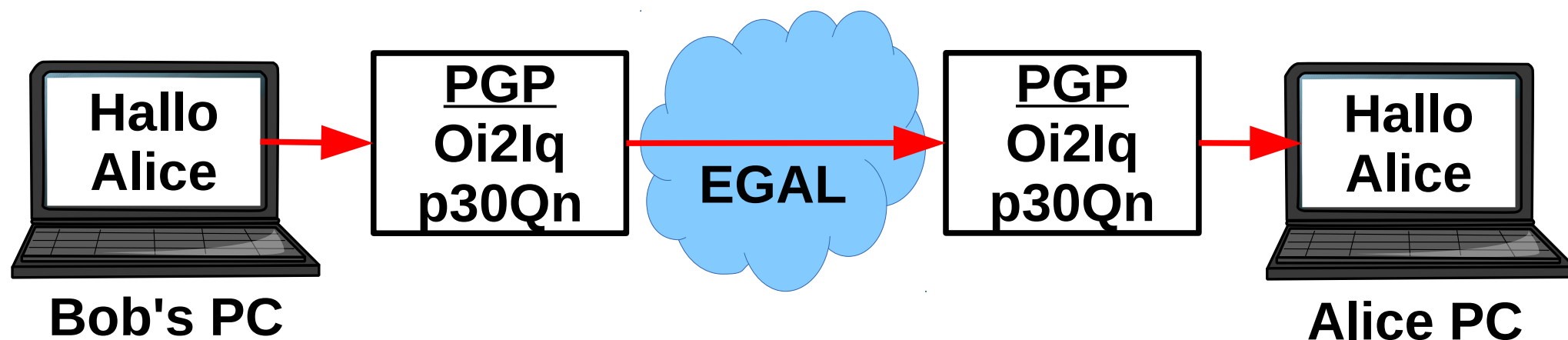
„klassische“ unzureichende
Verschlüsselungs-Möglichkeiten bei E-Mails



CryptoParty



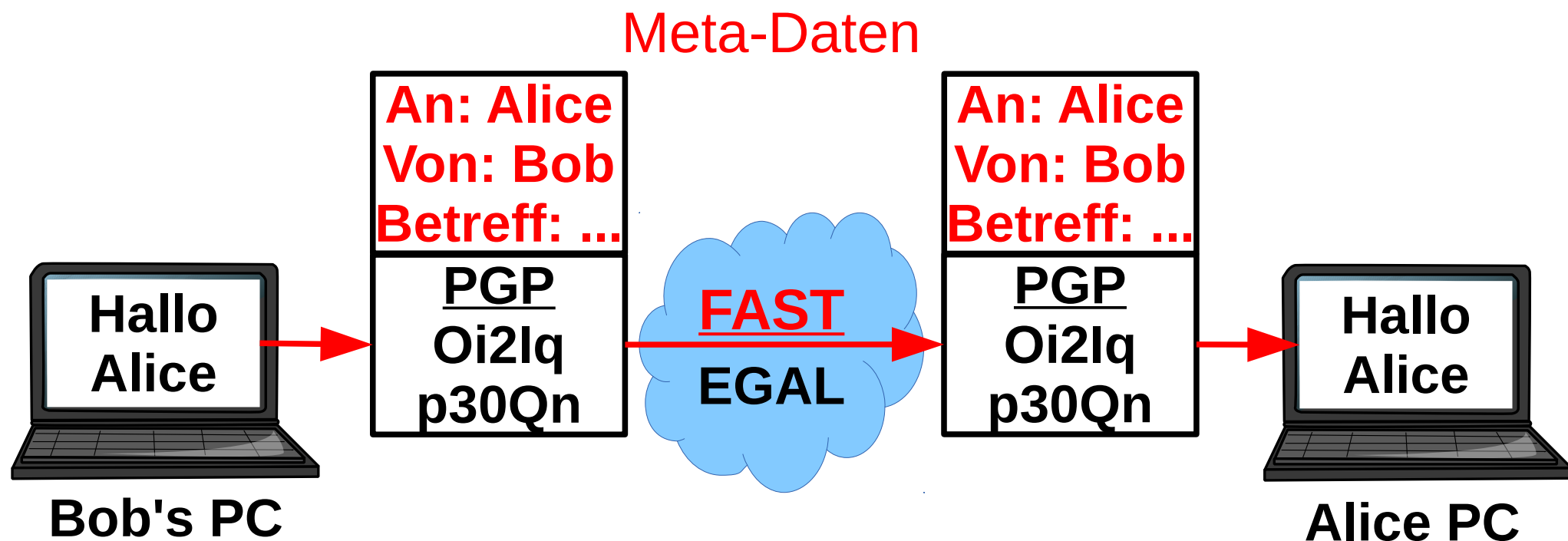
Ende-zu-Ende Verschlüsselung



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

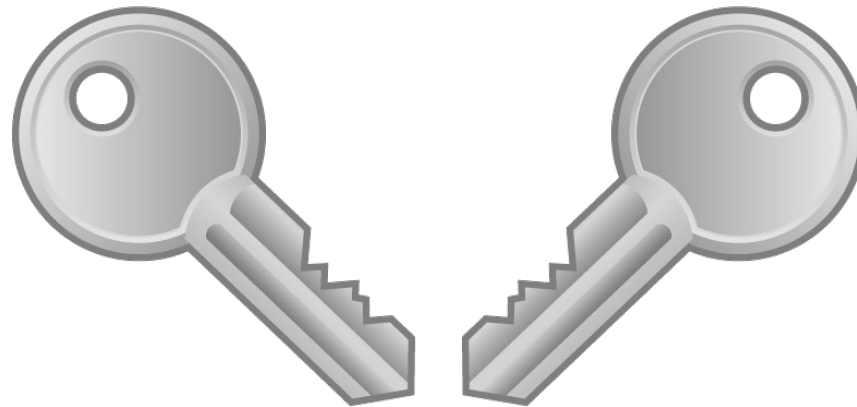
In Thunderbird:

Add-ons => Suchen (oben rechts) => Enigmail

CryptoParty



Öffentlicher und Privater Schlüssel Public Key / Private Key



Zwei Anwendungszwecke:
Verschlüsseln
Signieren

CryptoParty



Verschlüsseln

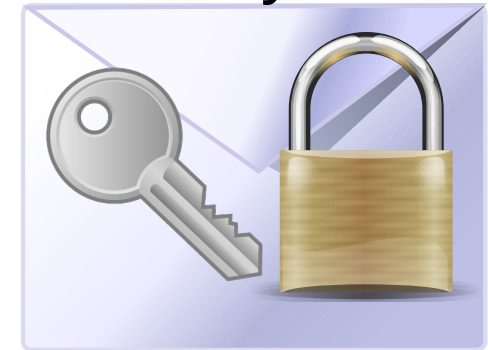
Alice (Absender)
Public Key von Bob



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

kein Fremder kann mitlesen

Schutz vor Überwachung

Mailinglisten: kompliziert

Signieren

Authentizität

echt / nicht verändert

ggf. Beweismittel

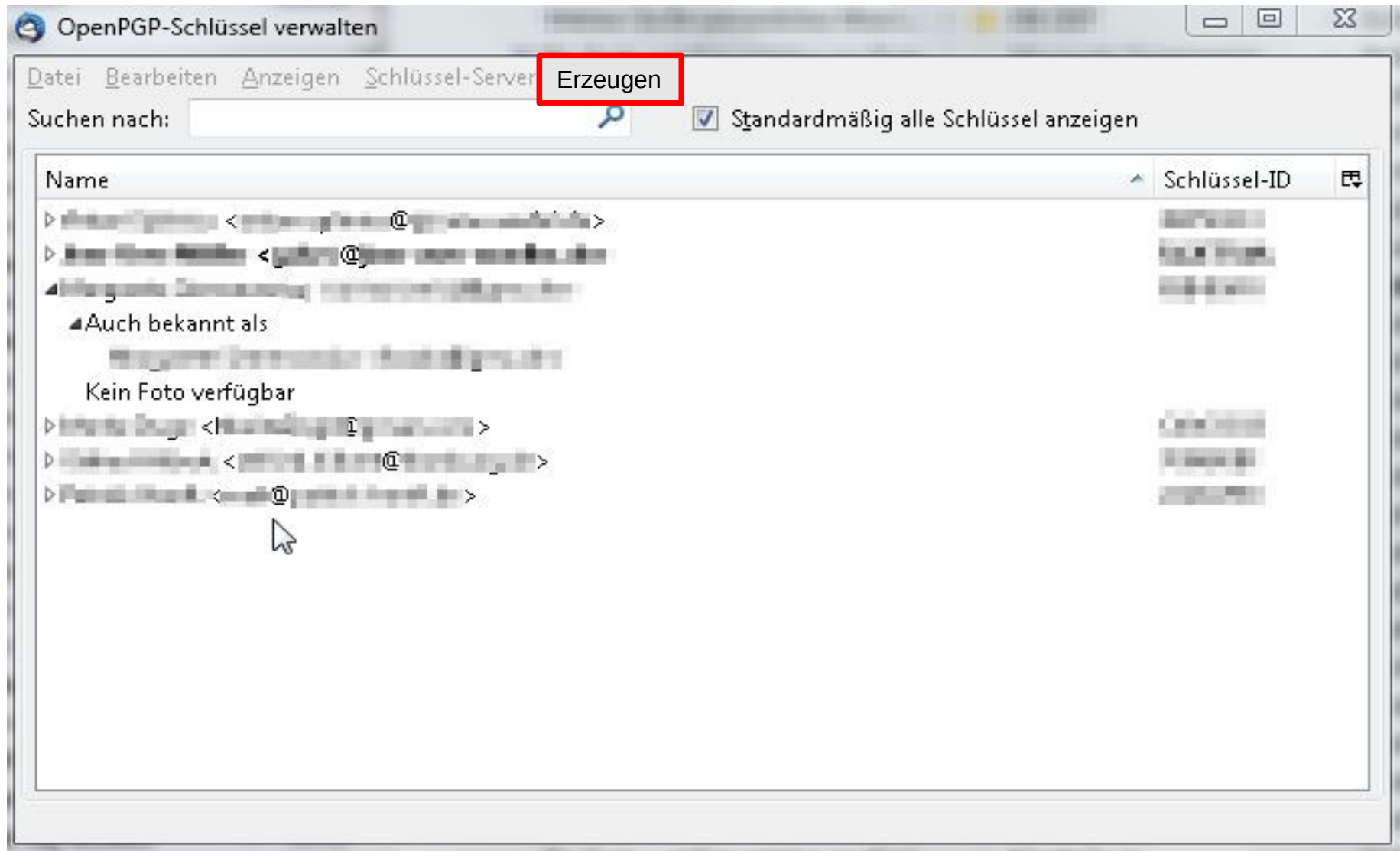
Mailinglisten: einfach

**kann jeweils einzeln oder
kombiniert verwendet werden**

CryptoParty



Enigmail



CryptoParty



Enigmail

OpenPGP-Schlüssel erzeugen

Benutzer-ID

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase Passphrase (wiederholen)

Kommentar

Schlüssel läuft ab in Jahren Schlüssel läuft nie ab

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.

CryptoParty



Enigmail

OpenPGP-Schlüssel erzeugen

Benutzer-ID

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase Passphrase (wiederholen)

Kommentar

Schlüsselstärke

Algorithmus

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.

CryptoParty



Enigmail

Primäre Benutzer-ID

Schlüssel-ID

Typ

Schlüsselgültigkeit

Besitzervertrauen

Fingerabdruck

Weitere Benutzer-ID	Gültig
Julius Zeidler (ccc) <chaos@zeidlos.de>	absolut

Schlüssel...	ID	Algorit...	Stä...	Erzeugt	Ablaufda...	Verwendung
Primär...	0x8BB1F669	RSA	4096	12.07.10	11.07.15	Unterschreiben, Beglaubigen, Authentifizieren
Unters...	0x58A59D89	RSA	4096	12.07.10	11.07.15	Verschlüsseln

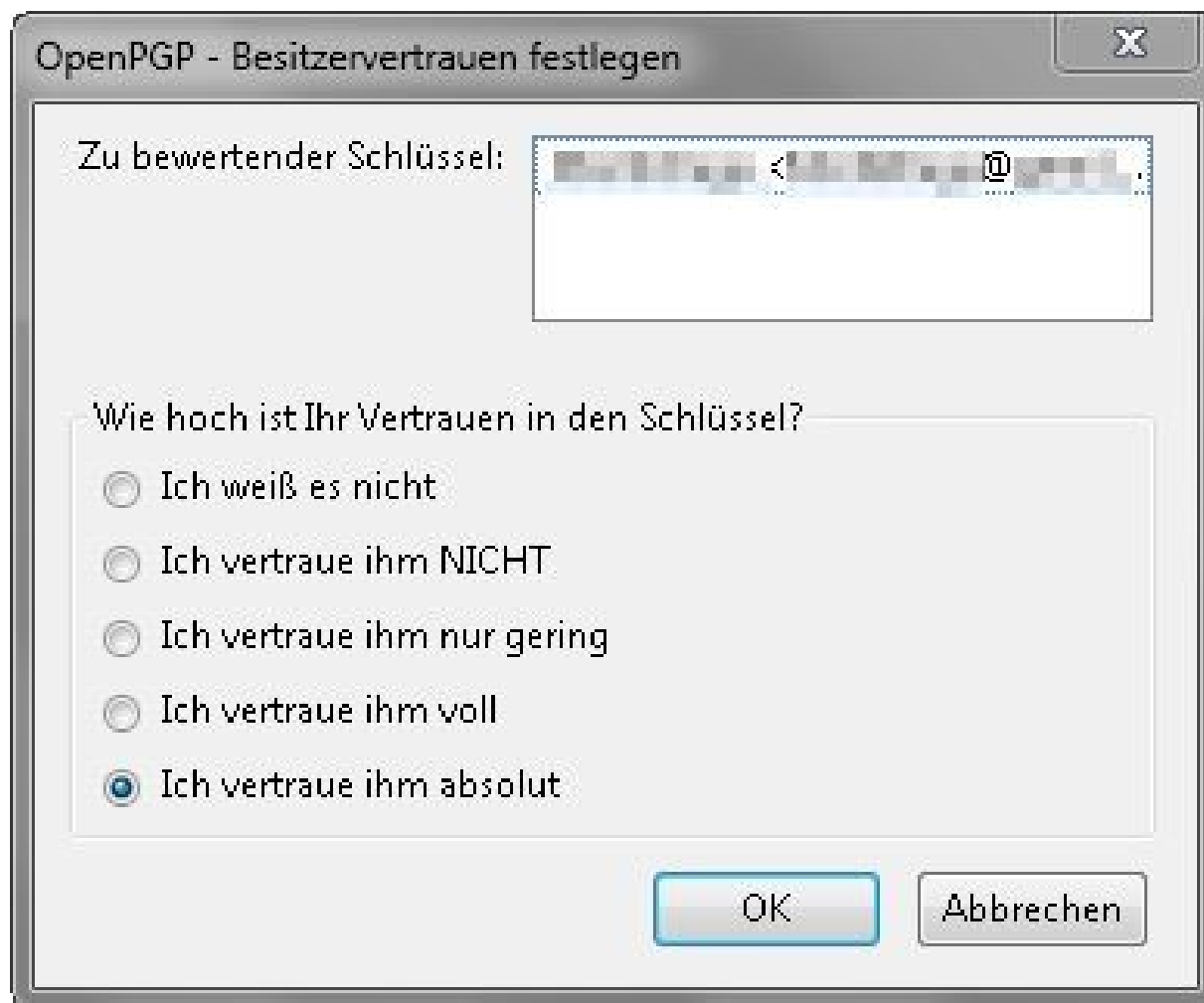
Aktion wählen... ▾

Schließen

CryptoParty



Vertrauensstufen für fremde Schlüssel in Enigmail



CryptoParty



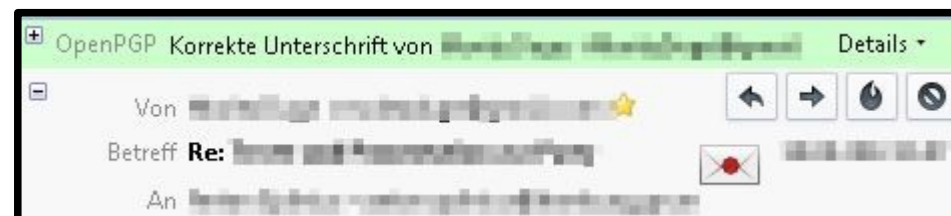
Vertrauensstufen für fremde Schlüssel in Enigmail

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.

www.kolahilft.de/cryptoparty
WLAN: BETAHAUS
KEY: betahaus10?

CryptoParty



Quellen

Abbildungen von:

<https://openclipart.org>

<https://commons.wikimedia.org>

CryptoParty

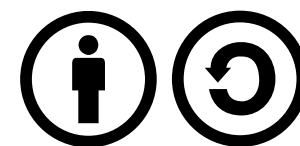


Folien-Lizenz

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

Alle Interessierten dürfen diese Folien unter den Bedingungen der „Creative Commons“ by-sa Lizenz nutzen. Weitere Informationen dazu unter:

<https://creativecommons.org/licenses/by-sa/3.0/de/>



Sie dürfen:

- das Werk bzw. den Inhalt vervielfältigen, verbreiten und öffentlich zugänglich machen
- Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anfertigen
- das Werk kommerziell nutzen