

Verschlüsselung des E-Mail-Verkehrs mit GnuPG

Christian Koch

`christian_koch@gmx.de`

5. Mai 2007

1 Grundlagen

2 GNUMPG

3 ENIGMAIL

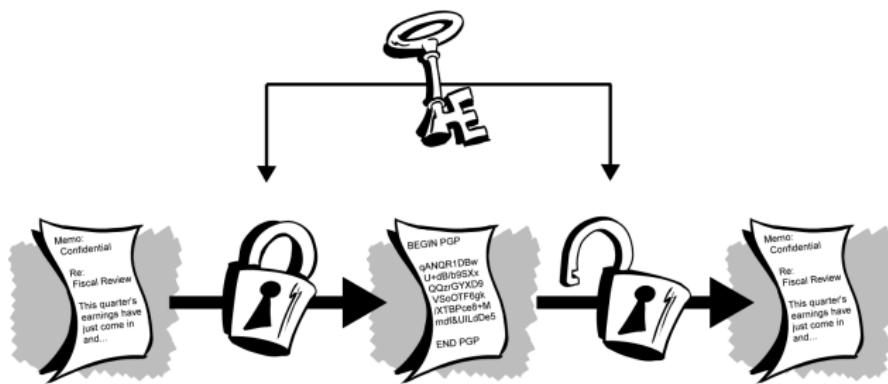
4 Schlußbemerkungen

5 Lizenz

Notwendigkeit der E-Mail-Verschlüsselung

- Privatsphäre
- §110 Telekommunikationsgesetz: automatisiertes Überwachen der Telekommunikation durch berechtigte Stellen
- Abfangen von E-Mail-Nachrichten im lokalen Netz
- viele E-Mail-Nachrichten konzentriert auf Festplatte gespeichert

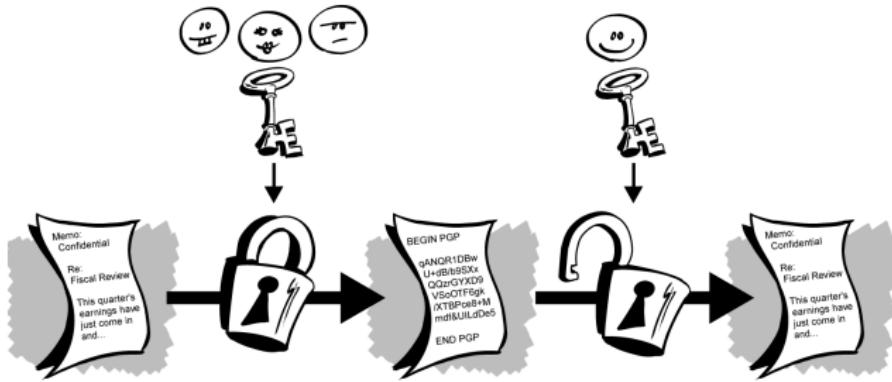
Prinzip der symmetrischen Chiffrierung



© PGP Corporation.

Analogon: Tresor, in den nur diejenigen etwas hineinlegen oder herausholen können, die den passenden Schlüssel besitzen

Prinzip der asymmetrischen Chiffrierung



© PGP Corporation.

Analogon: Briefkasten, in den jeder etwas einwerfen kann, aber nur derjenige, der den richtigen Schlüssel besitzt, kann es wieder herausholen

Praxis der asymmetrischen Chiffrierung

Voraussetzungen

- jeder Teilnehmer erzeugt einmalig ein Schlüsselpaar
- Schlüsselpaar besteht aus öffentlichen und privaten Schlüssel
- öffentliche Schlüssel werden untereinander ausgetauscht und authentifiziert
- privater Schlüssel wird geheimgehalten

Anwendung

- Verschlüsselung mit öffentlichen Schlüssel des Empfängers
- Entschlüsselung mit privatem Schlüssel des Empfängers
- Signieren mit privatem Schlüssel des Absenders
- Signaturüberprüfung mit öffentlichem Schlüssel des Absenders

Was ist GNUPG?

Der GNU Privacy Guard ist ein OpenPGP-kompatibles¹ Programm ...

- zur Erzeugung und Verwaltung asymmetrischer Schlüsselpaare,
- zum Ver- und Entschlüsseln von Dateien,
- zum Signieren und Verifizieren von Dateien,
- zum Beglaubigen (= Signieren) fremder Schlüssel.

Der GNU Privacy Guard bietet keine ...

- grafische Benutzeroberfläche (→ Enigmail, Seahorse, KMail, KGpg),
- Echtzeitverschlüsselung (→ ssh).

¹<http://www.imc.org/rfc2440>

OpenPGP-Schlüssel

- Algorithmen und Schlüssellängen nach Sicherheitsbedürfnis wählbar
- privater Schlüssel durch Paßwort oder besser „Paßsatz“ geschützt
- Gültigkeit begrenzt durch zeitliche Frist oder Widerruf
- Austausch öffentlicher Schlüssel mittels Keyservern², die sich untereinander synchronisieren

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2.0.3 (FreeBSD)

```
mQELBE0gWmcBCADO1Qh3ik7sNjSQ1mr+xgLF8FOEwE8e12F03gtYjoCQTvu/316H  
jAbMGJ638eqwYrpRTfZ8CDxIMwWOC2Vk51BLNwewlz+2ec6fmMkZ1ElxWIDp51qF  
[...]  
lwN5JTLSzmkp6twGMQoennrVfKbKXIptTd6k8SBw60A1yR4w0KOwMrWma5KIwYEp  
iF0jkJEkpmreqc8PO6w83QBHNBySXfLVJUz8A==  
=6RT9
```

-----END PGP PUBLIC KEY BLOCK-----

²z.B. <http://wwwkeys.de.pgp.net/>

Authentizität fremder Schlüssel

- Ist ein vom Keyserver gelieferter Schlüssel authentisch?

```
Type bits/keyID      Date        User ID
pub  2048R/1BB8F7FC  2005-12-14  Christian Koch <christian_koch@gmx.de>
                                         Christian Koch <info@christiankoch.de>
Fingerprint=1345 5E5E 297F DFEF 464F  6AE9 CA9F B7AD 1BB8 F7FC
```

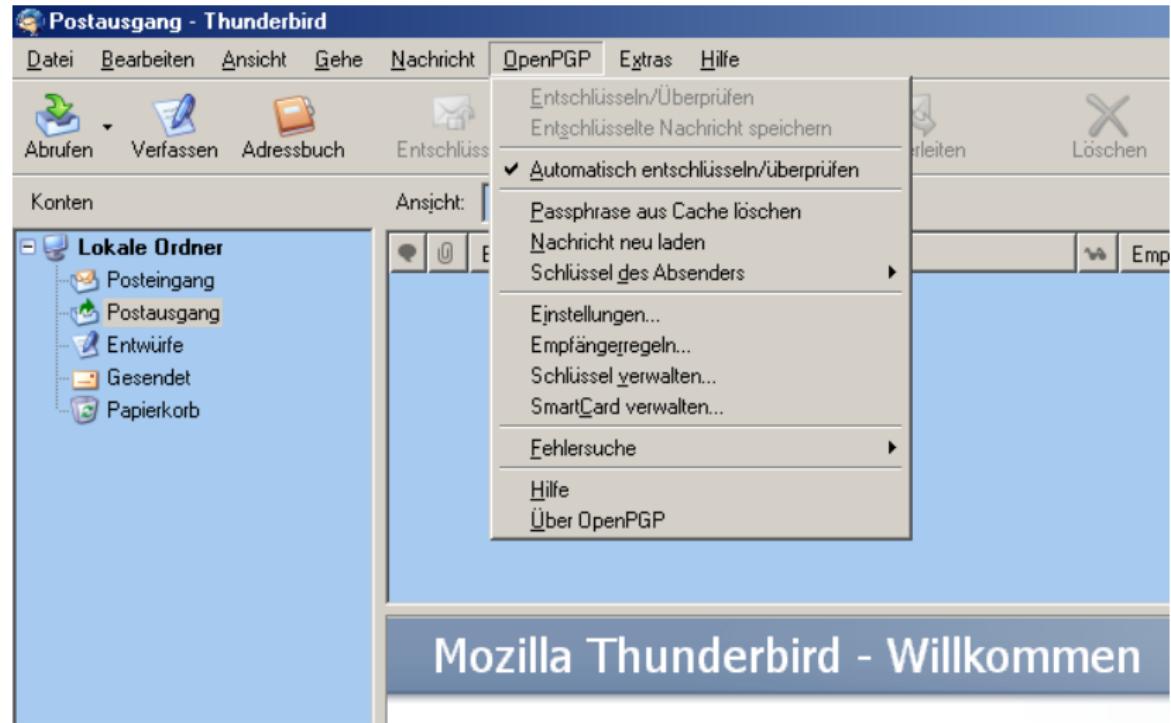
- Schlüssel wird gültig durch ...

- Beglaubigen des Schlüssels nach Prüfung der Authentizität u. a. durch digitalen Fingerabdruck
- Beglaubigungen durch vertraute Schlüssel (sog. web of trust)

Was ist ENIGMAIL?

- grafische Benutzeroberfläche für GnuPG
- Erweiterung für Thunderbird Mail und SeaMonkey
- offener Quelltext und damit für viele Betriebssysteme verfügbar
- unterstützt Verschlüsselung und digitale Unterschrift in E-Mails
- integrierte Schlüsselverwaltung

OpenPGP-Menüeinträge

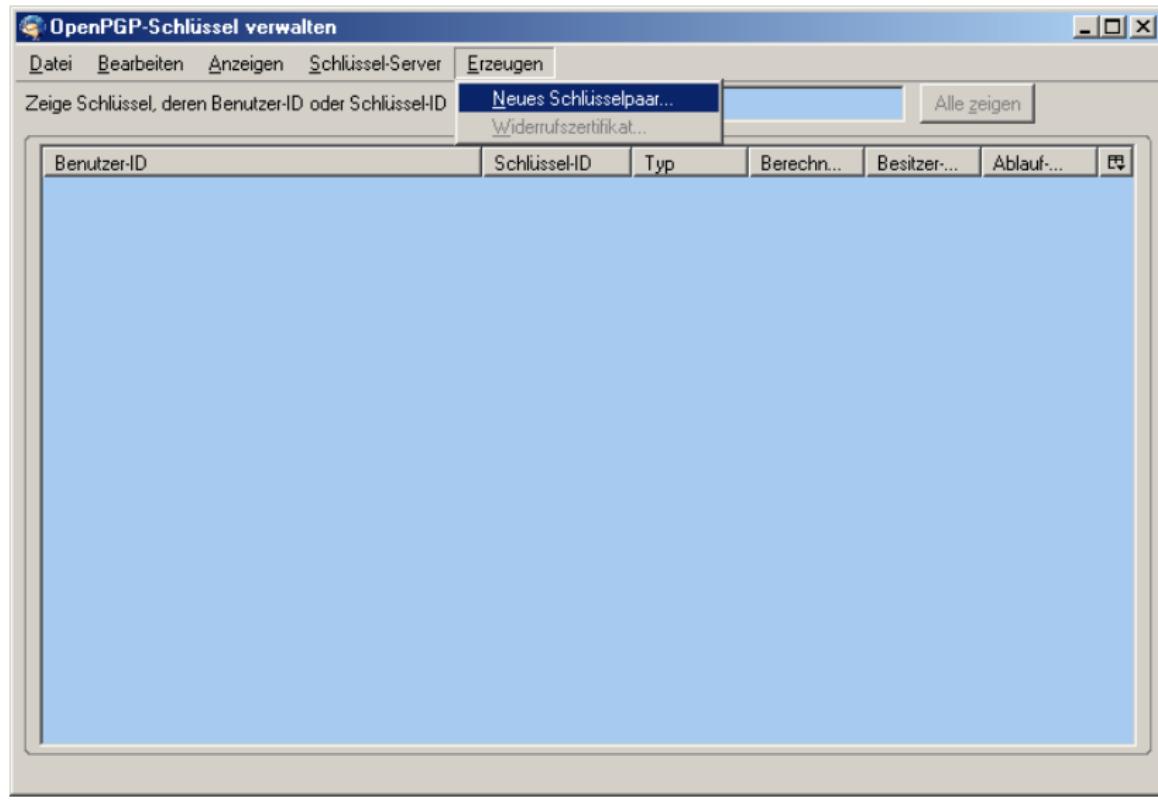


Mozilla Thunderbird - Willkommen

C3LE



Schlüsselverwaltung



c3le

Schlüsselpaar erzeugen (1/2)

OpenPGP-Schlüssel erzeugen

Benutzer-ID Christian Koch <christian_koch@gmx.de> - christian_koch@gmx.de

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase: Passphrase wiederholen:

Kommentar:

Ablauf-Datum:

Schlüssel läuft ab in: Jahren Schlüssel läuft nie ab

Konsole zum Erzeugen eines Schlüssels

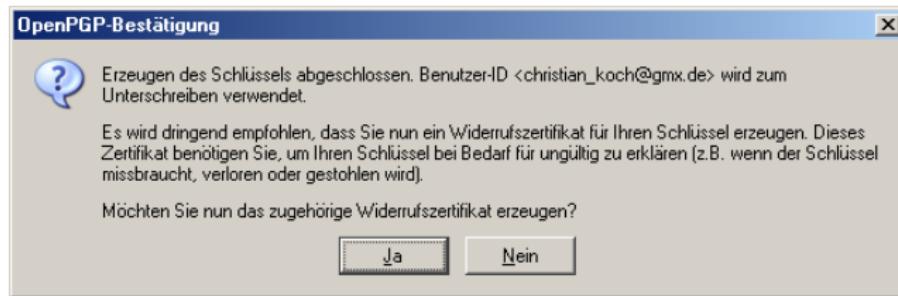
ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.



Schlüsselpaar erzeugen (2/2)

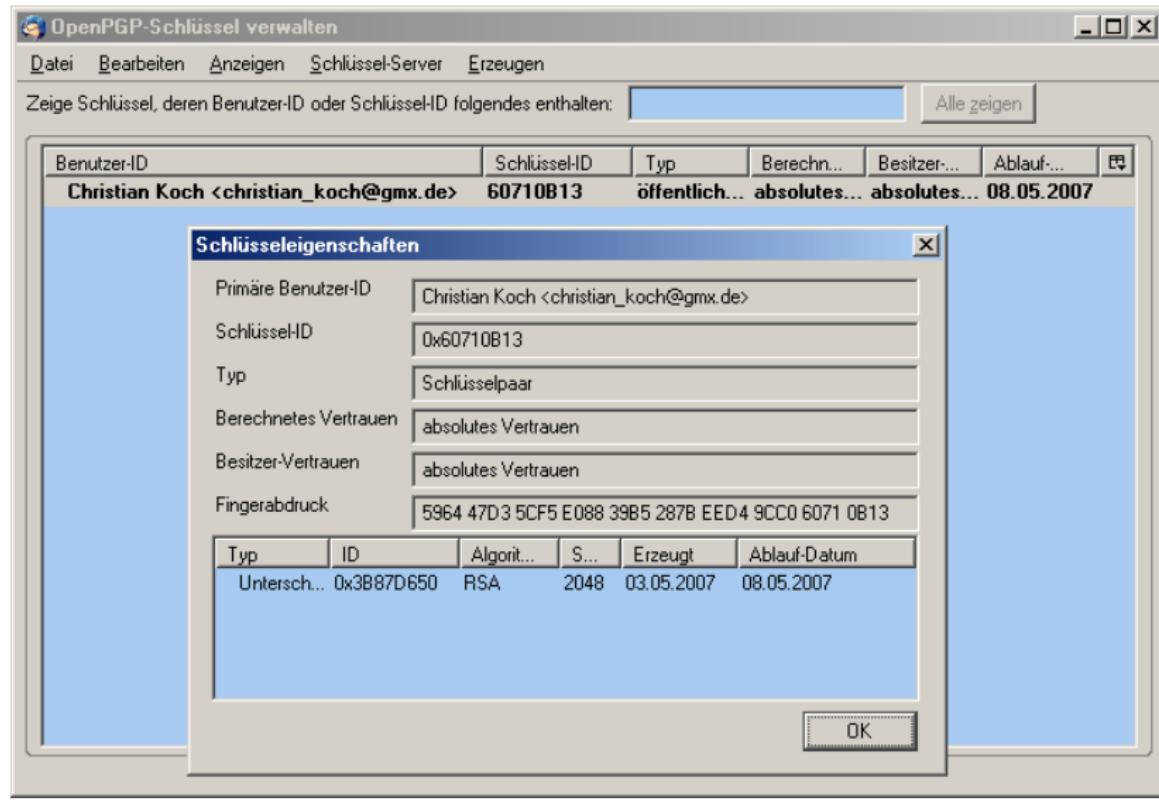
- Pseudonym als Identität möglich
- später weitere Identitäten (E-Mail-Adressen, Fotos) einem Schlüssel zuordenbar
- Gültigkeitsdauer nach Sicherheitsbedürfnis und Bequemlichkeit wählen

Widerrufszertifikat erstellen



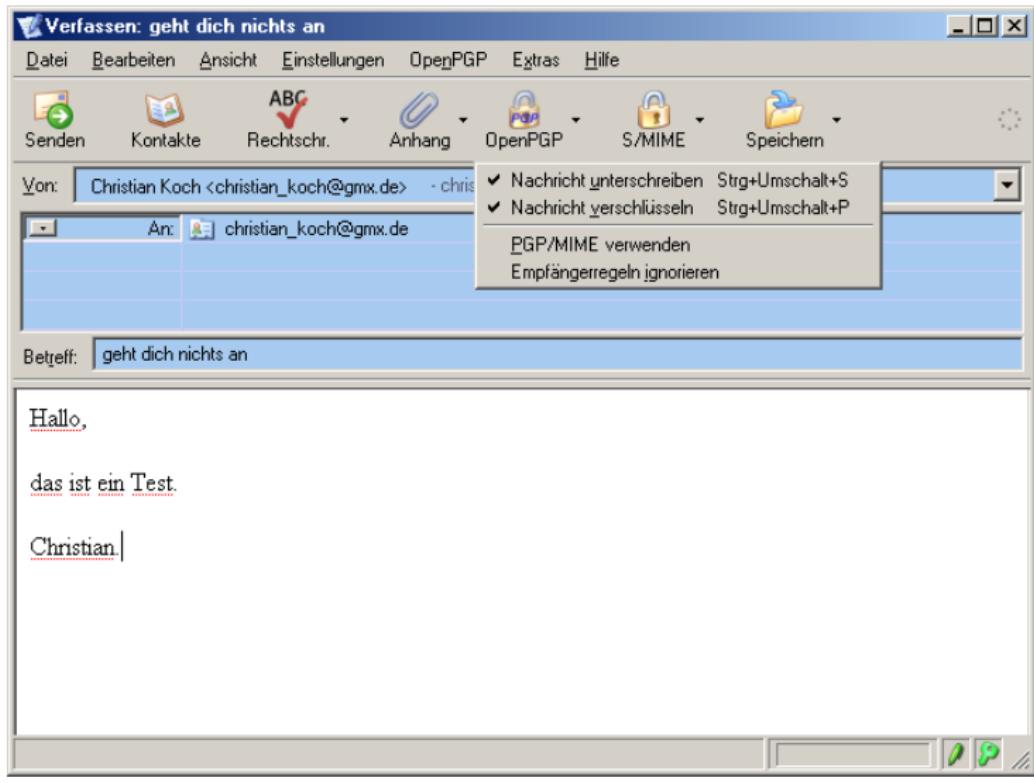
Das Widerrufszertifikat muß sicher vor fremden Zugriff abgespeichert werden. Durch Hochladen des Zertifikats auf einen Keyserver wird der Schlüssel unwiderruflich als zurückgezogen markiert. Verwendung z. B. bei Verlust oder Aufdeckung des privaten Schlüssels, bei Ungültigwerden von E-Mail-Adressen.

Schlüsseleigenschaften des erzeugten Schlüsselpaares



cole

Verfassen einer verschlüsselten Nachricht



Anzeigen einer entschlüsselten Nachricht

The screenshot shows the Thunderbird email client interface. The window title is "geht dich nichts an - Thunderbird". The menu bar includes Datei, Bearbeiten, Ansicht, Gehe, Nachricht, OpenPGP, Extras, and Hilfe. The toolbar contains icons for Abrufen, Verfassen, Adressbuch, Entschlüsseln, Antworten, Allen antworten, Weiterleiten, Löschen, Junk, and Drucken. A green status bar at the top indicates "OpenPGP: Entschlüsselte Nachricht; Korrekte Unterschrift von Christian Koch <christian_koch@gmx.de>". The message list shows one item: "Betreff: geht dich nichts an" with "Von: Christian Koch <christian_koch@gmx.de>". Below the message list, the message content is displayed:

Hallo,

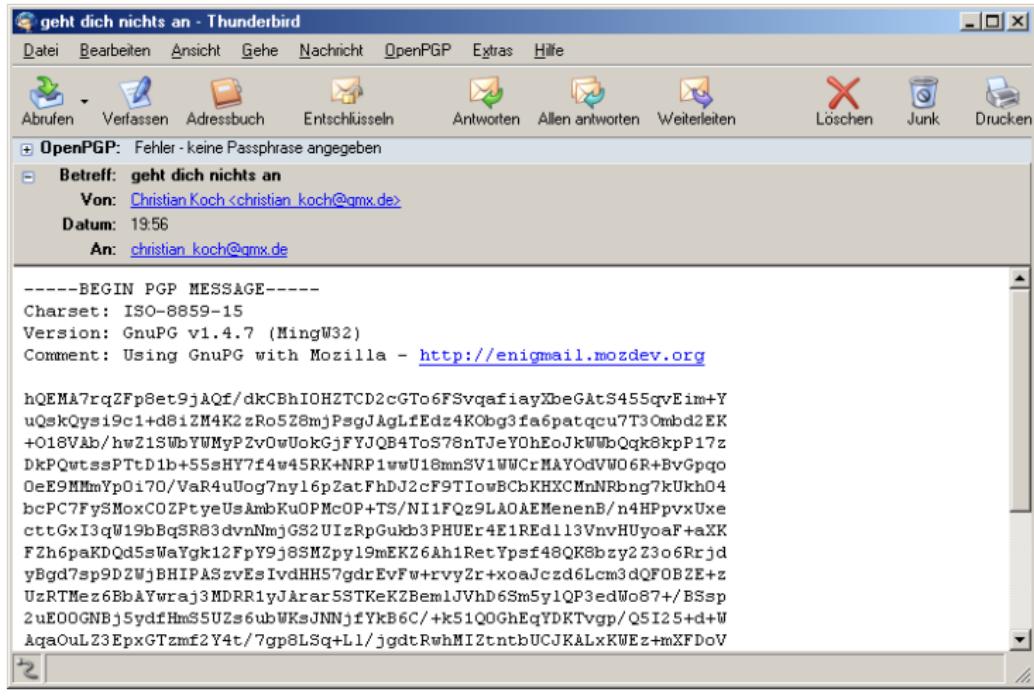
das ist ein Test.

Christian.

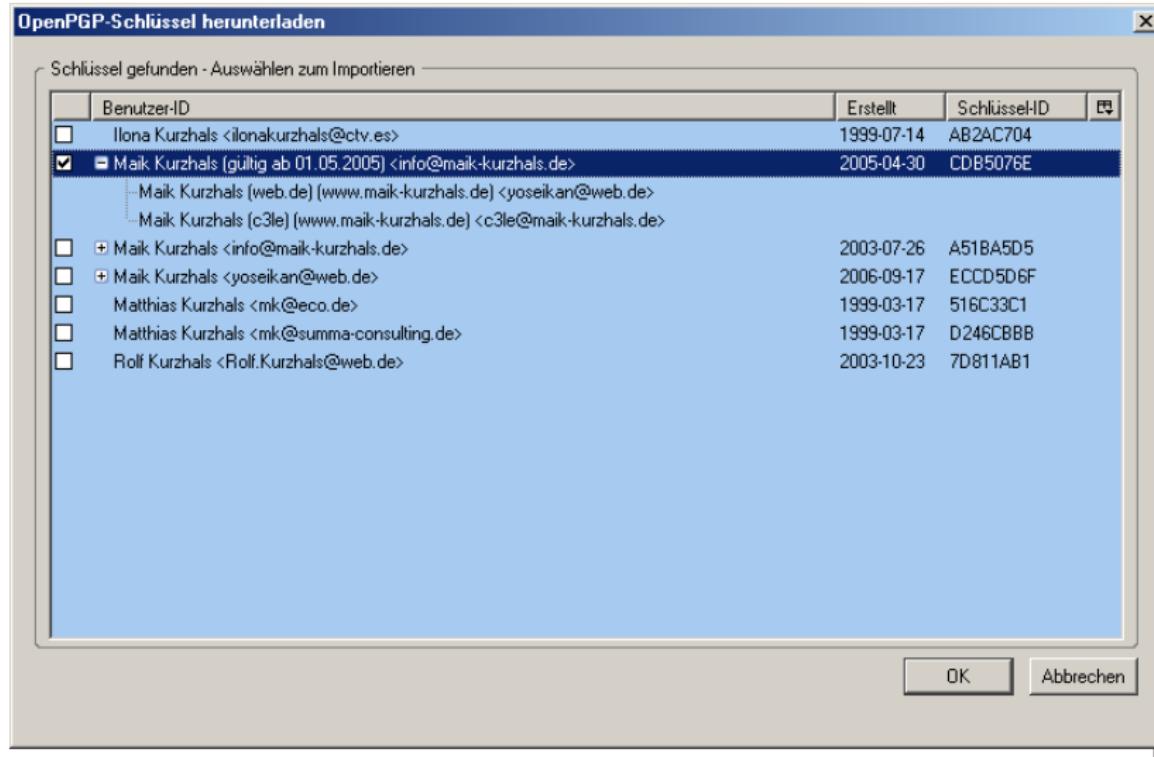
The bottom right corner of the message area features two small icons: a blue pen and a yellow key. The status bar at the bottom includes icons for file operations like Open, Save, Print, and Find, along with the GnuPG logo and the word "ENIGMAIL".

Anzeigen einer nicht entschlüsselbaren Nachricht

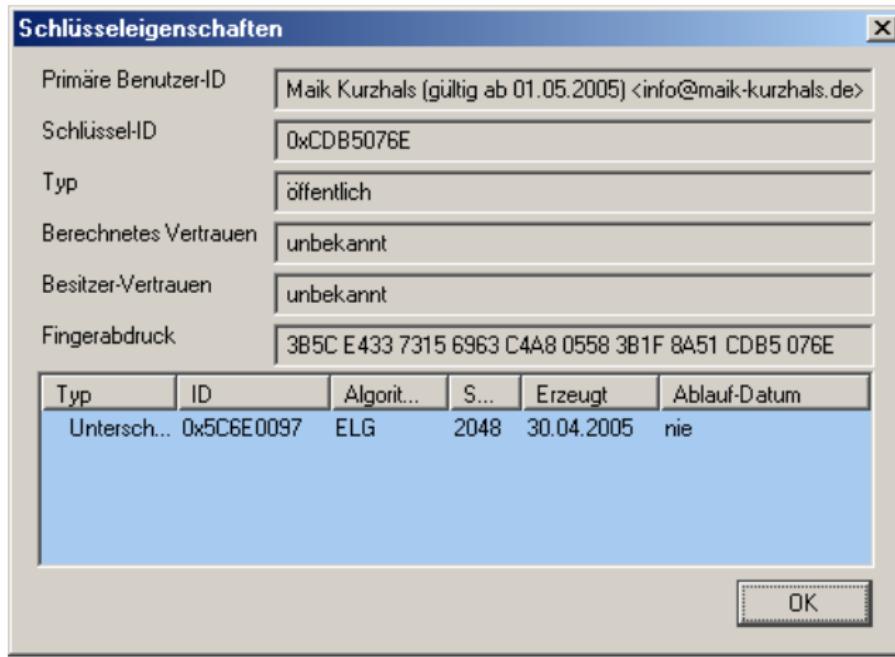
Achtung: Betreffzeile wird nicht verschlüsselt!



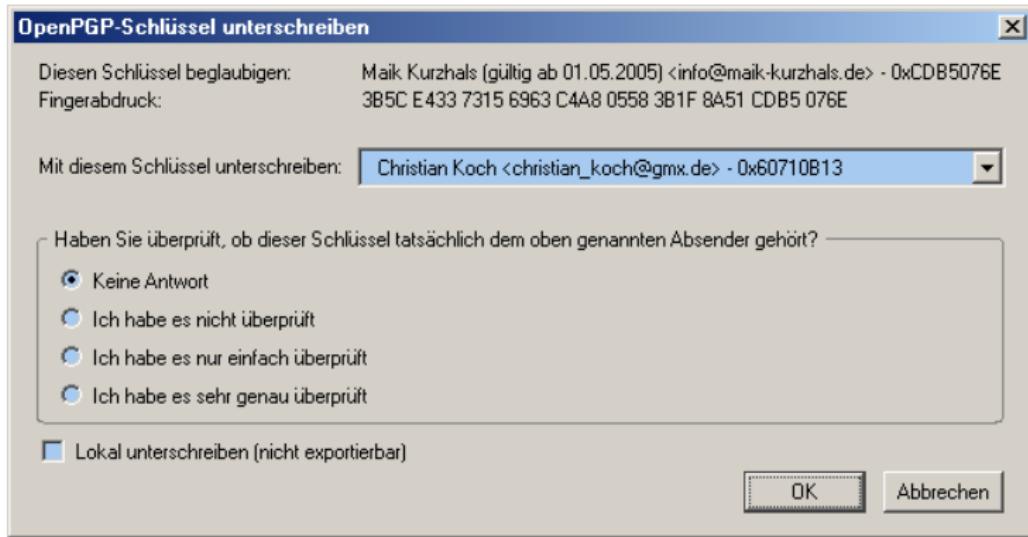
Import eines Schlüssels vom Keyserver



Schlüsseleigenschaften eines unbeglaubigten Schlüssels



Beglaubigen eines Schlüssels



Schlußbemerkungen

- realistische Schlüsselgrößen benutzen: Niemand baut eine Tresortür als Wohnungstür ein!
- privaten Schlüssel in einer geschützten Umgebung verwenden (eigener Computer, ggf. Chipkarte), siehe „Bundestrojaner“
- Sicherheitslücken durch Updates regelmäßig schließen
- keine Links in E-Mails anklicken, ggf. anonym surfen³
- Verbindungsdaten auch durch Verschlüsselung weiterhin erkennbar, siehe Vorratsdatenspeicherung, ggf. Mixmaster-Remailer benutzen

³z.B. <http://tor.eff.org/>

Lizenz



Dieser Inhalt ist unter einem Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen Lizenzvertrag lizenziert. Um die Lizenz anzusehen, gehen Sie bitte zu

<http://creativecommons.org/licenses/by-sa/2.0/de/>
oder schicken Sie einen Brief an Creative Commons, 559 Nathan Abbott Way,
Stanford, California 94305, USA.