Verschlüsselung des E-Mail-Verkehrs mit GnuPG

Christian Koch Eric Goller

Chaostreff Leipzig

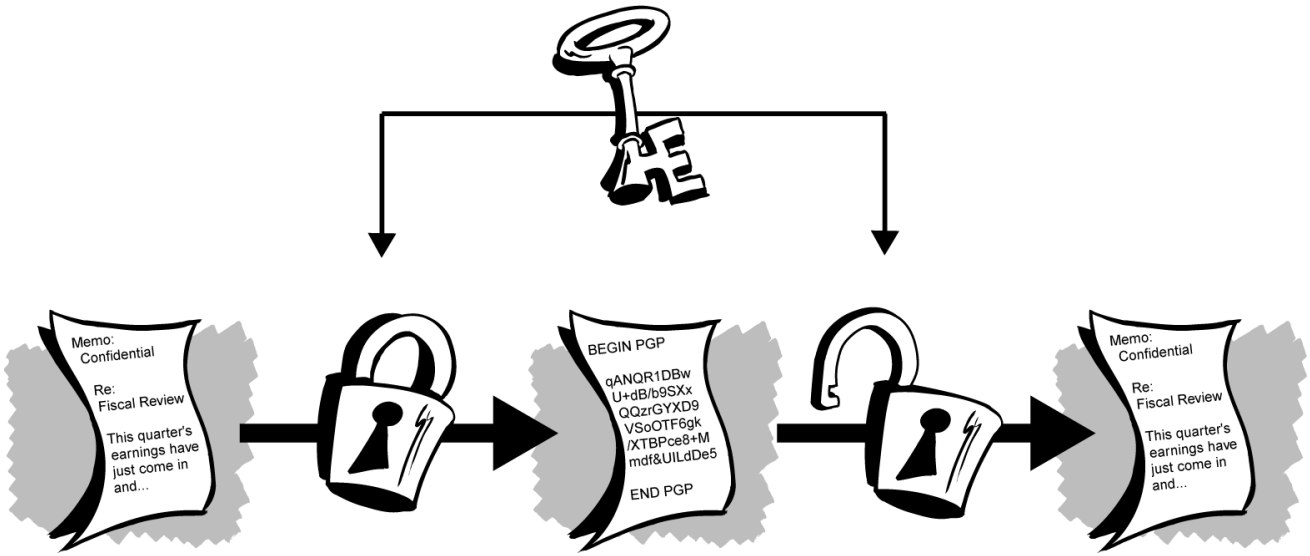
7. Juni 2008

Agenda

Notwendigkeit der E-Mail-Verschlüsselung

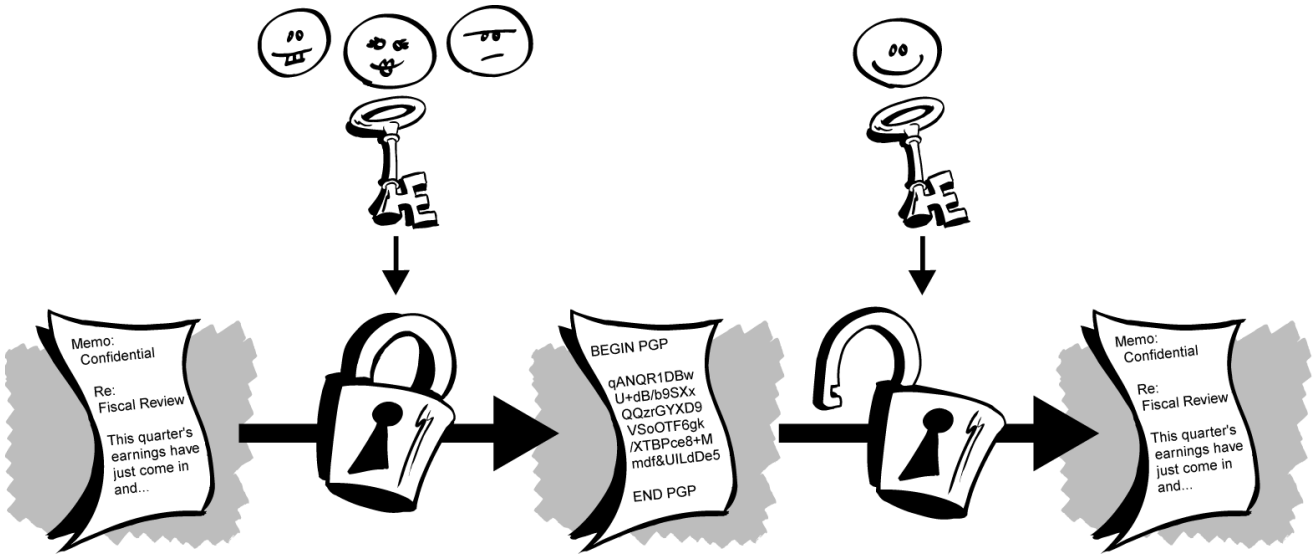
- Privatsphäre
- §110 Telekommunikationsgesetz: automatisiertes Überwachen der Telekommunikation durch berechtigte Stellen
- Abfangen von E-Mail-Nachrichten im lokalen Netz
- viele E-Mail-Nachrichten konzentriert auf Festplatte gespeichert
- aktuelle Entscheidung StB 34/07 des BGH: Verschlüsselung von E-Mails begründet keinen dringenden Tatverdacht

Prinzip der symmetrischen Chiffrierung



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

Prinzip der asymmetrischen Chiffrierung



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

OpenPGP Geschichte

- 1991 wird PGP 1.0 von dem US-Amerikaner Phil Zimmermann geschrieben und als Freeware im USENET veröffentlicht
- 1993 beginnen Ermittlungen gegen Zimmermann wegen angeblichen Verstoßes gegen US-Exportkontrollgesetze, da PGP als militärische Waffe angesehen wird und PGP im Internet weltweit verfügbar ist
- 1996 werden die Ermittlungen ohne Angabe von Gründen eingestellt
- 1996 beschreibt RFC 1991 das Nachrichtenformat von PGP 2.6, welches RSA, IDEA und MD5 nutzt
- 1998 beschreibt RFC 2440 das OpenPGP-Nachrichtenformat ab PGP 5.0 und GnuPG
- 1999 erscheint GnuPG 1.0.0
- 2000 RSA-Patent läuft aus, GnuPG 1.0.3 mit RSA-Implementierung
- 2007 löst RFC 4880 den RFC 2440 ab

Was ist GnuPG?

Der GNU Privacy Guard ist ein OpenPGP-kompatibles[1] 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 ($\rightarrow$ Enigmail, Seahorse, KMail, KGpg),
- Echtzeitverschlüsselung ($\rightarrow$ ssh).

[1] http://www.imc.org/rfc4880

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 Keyservern[2], die sich untereinander synchronisieren

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.3 (FreeBSD)

mQELBEOgWmcBCADO1Qh3ik7sNjSQ1mr+xgLF8FOEwE8el2F03gtYjoCQTvu/3l6H
jAbMGJ638eqwYrpRTfZ8CDxIMwWOC2Vk5lBLNwew1z+2ec6fmMkZ1ElxWIDp51qF
[...]
lwN5JTLSzmkp6twGMQoennrVfKbKXIpTnd6k8SBw60A1yR4w0KOwMrWma5KIwYEp
iF0jkJEkpmreqc8PO6w83QBHNBpySXfLVJUz8A==
=6RT9
-----END PGP PUBLIC KEY BLOCK-----
```

[2] z. B. `http://wwwkeys.de.pgp.net/`

Authentizität fremder Schlüssel

- Ist ein vom Keyserver gelieferter Schlüssel authentisch?

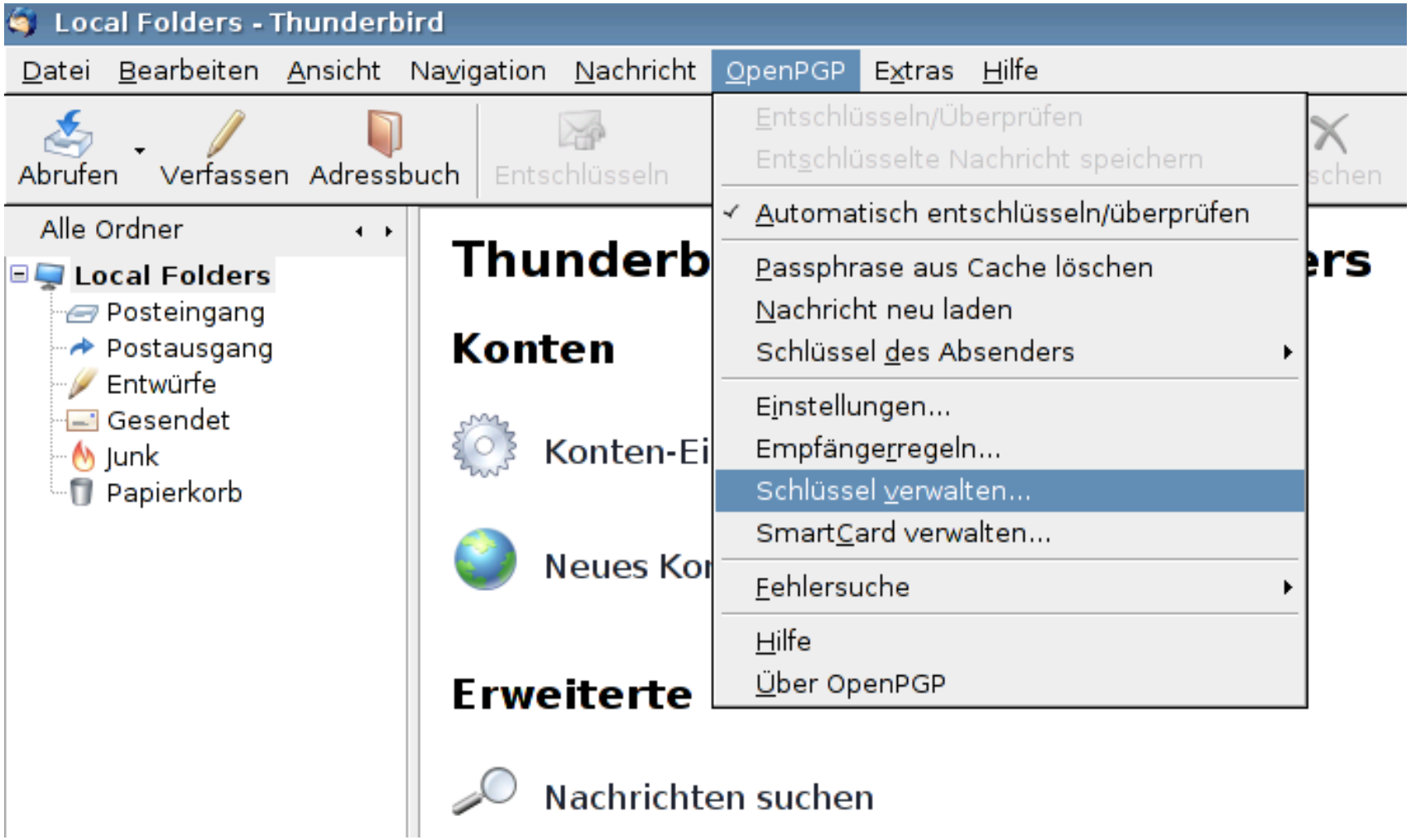
```
Type bits/keyID    Date       User ID
pub  2048R/1BB8F7FC 2005-12-14 Christian Koch <christian_koch@gmx.de>
                               Christian Koch <info@christiankoch.de>
 Fingerprint=1345 5E5E 297F DFEF 464F  6AE9 CA9F B7AD 1BB8 F7FC
```

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

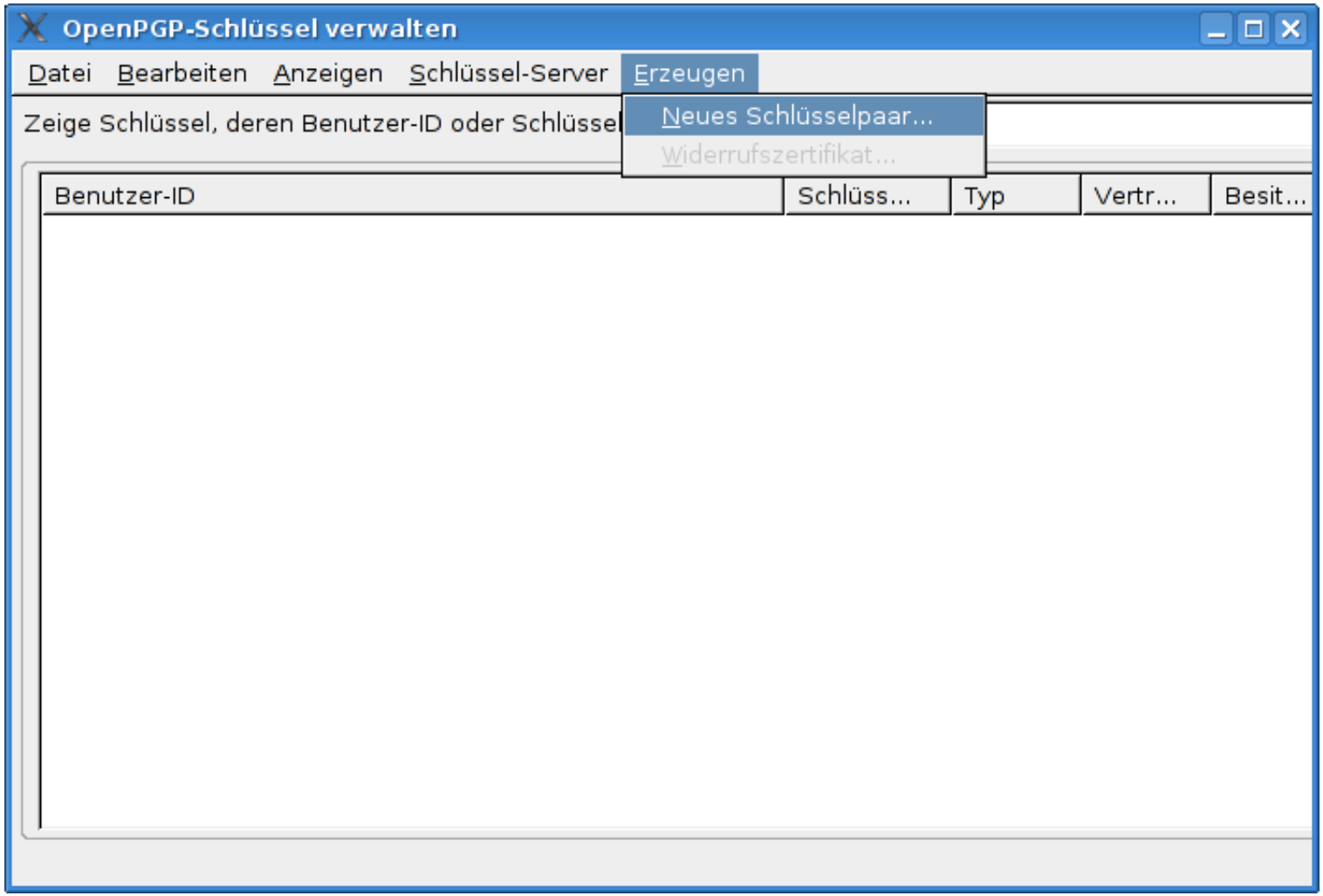
Was ist ENIGMAIL?

- 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

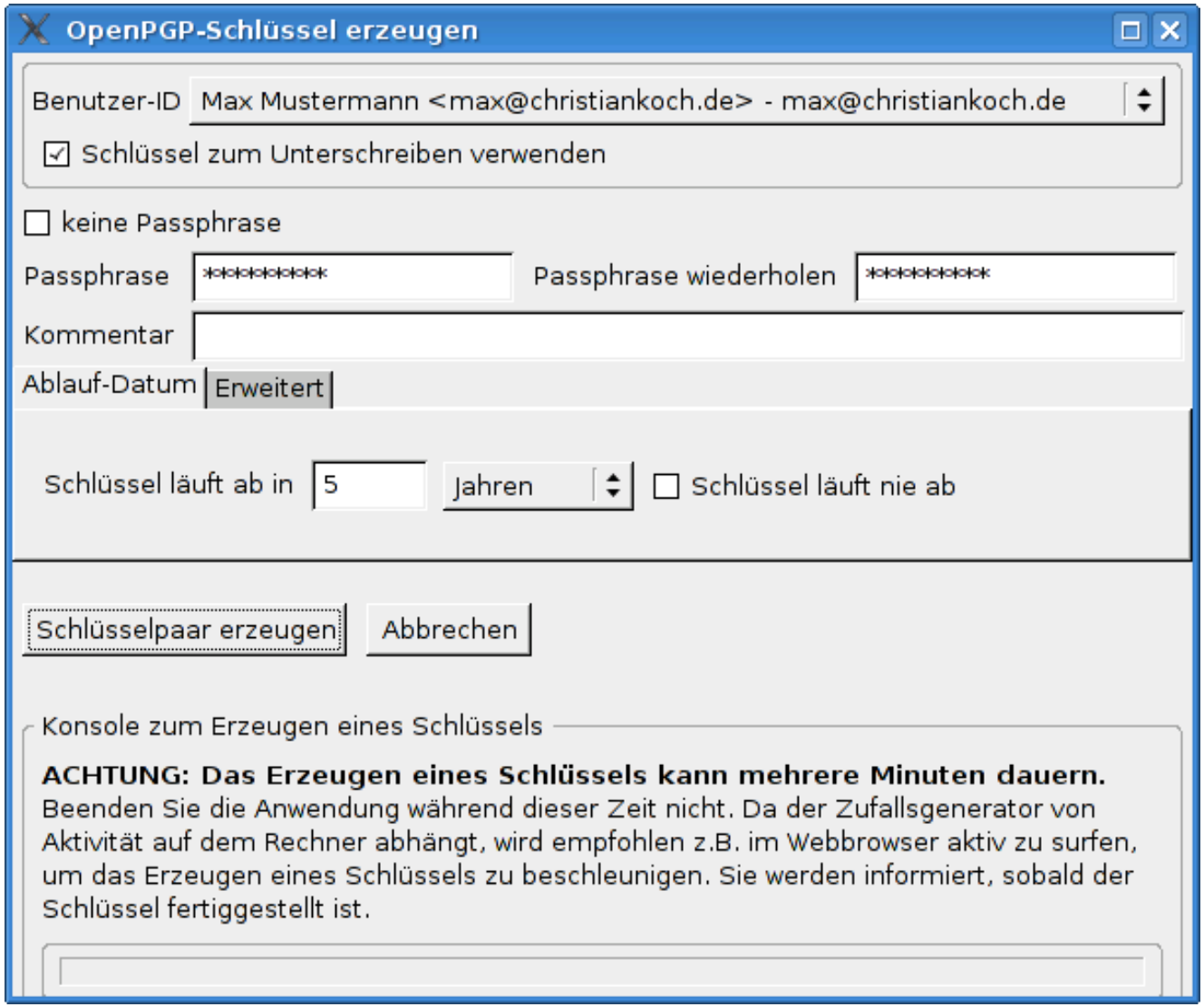
OpenPGP-Menüeinträge



Schlüsselverwaltung



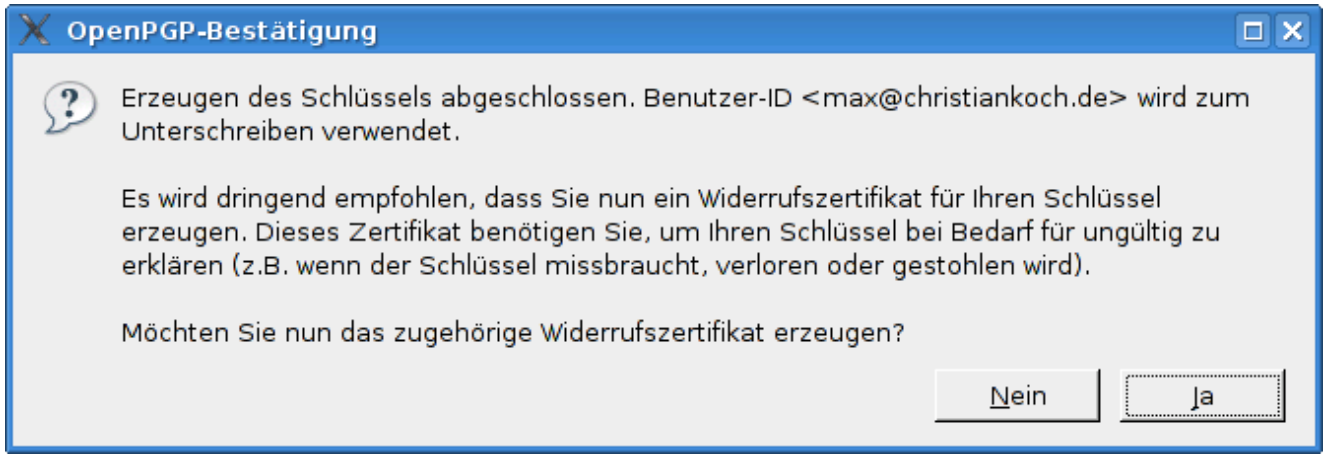
Schlüsselpaar erzeugen (1/2)



Schlüsselpaar erzeugen (2/2)

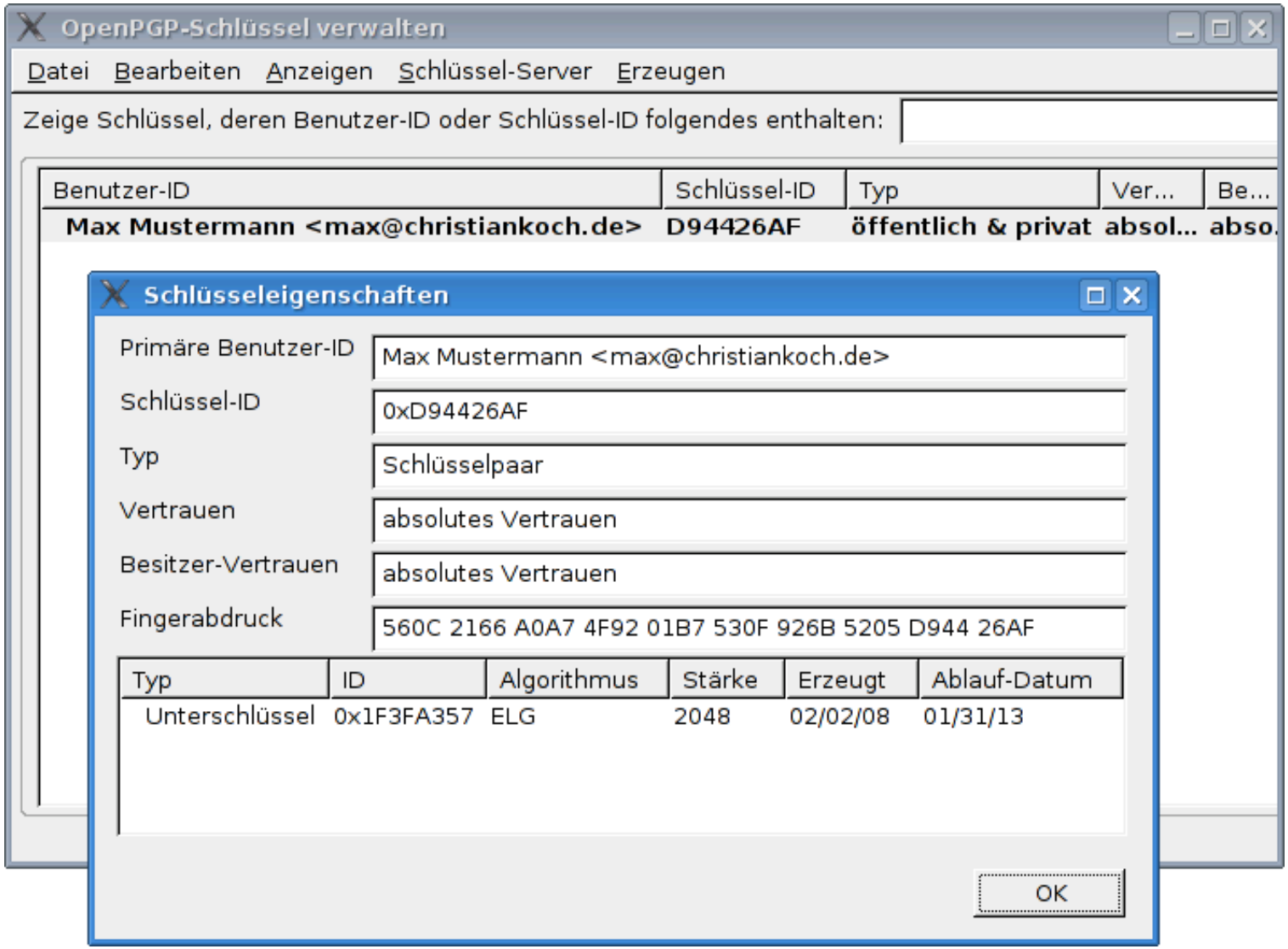
- Pseudonym als Identität möglich
- später weitere Identitäten (E-Mail-Adressen, Fotos) einem Schlüssel zuordenbar
- Verknüpfung von Identitäten durch Zuordnung zu einem Schlüssel nicht immer sinnvoll
- Gültigkeitsdauer nach Sicherheitsbedürfnis und Bequemlichkeit wählen

Widerrufszertifikat erstellen

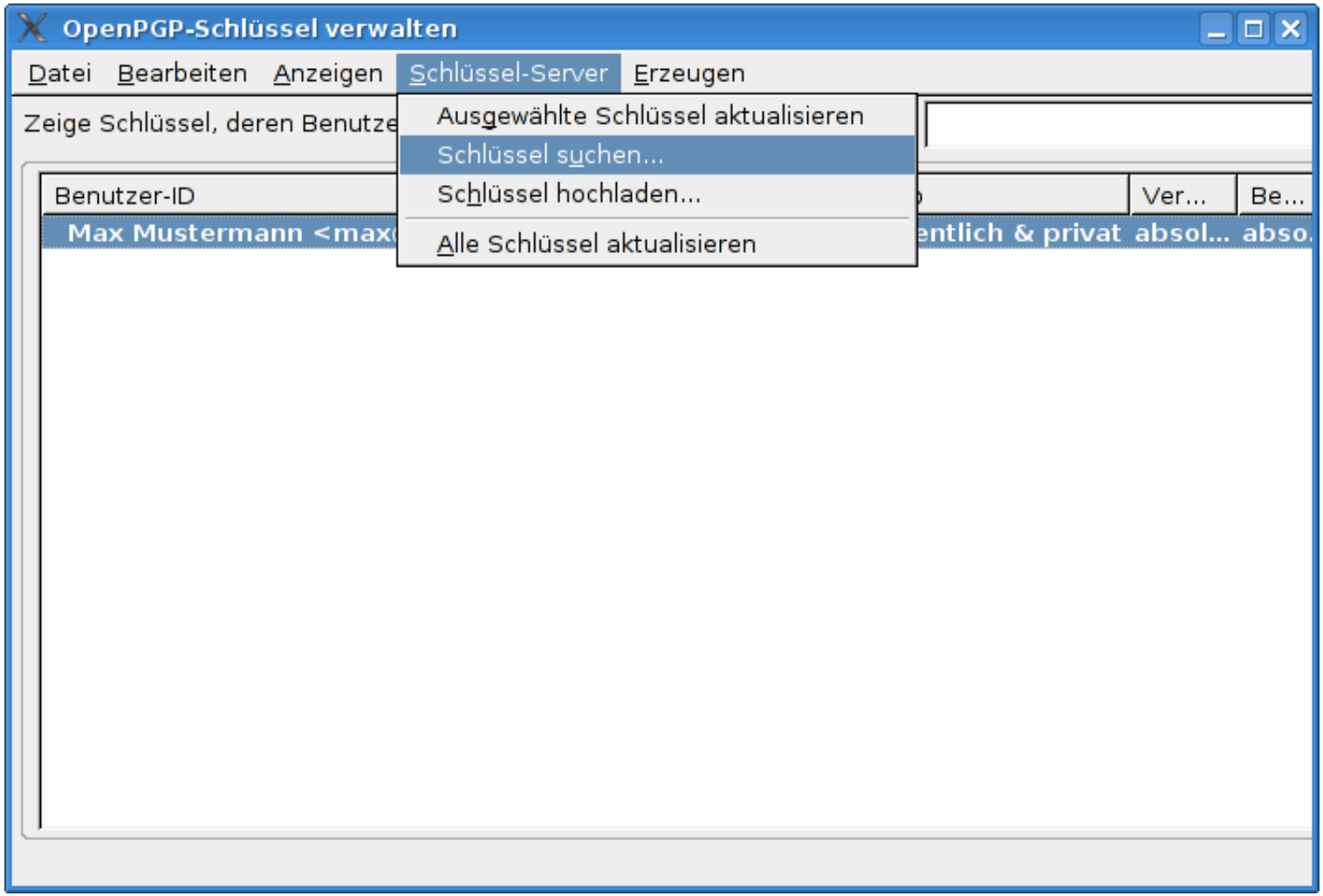


Das Widerrufszertifikat muß sicher vor fremden Zugriff abgespeichert werden. Durch Hochladen des Zertifikats auf einen Keyserver wird der Schlüssel unwiderruflich als zurückgezogen markiert. Verwendung z. B. bei Verlust oder Aufdeckung des privaten Schlüssels, bei Ungültigwerden von E-Mail-Adressen.

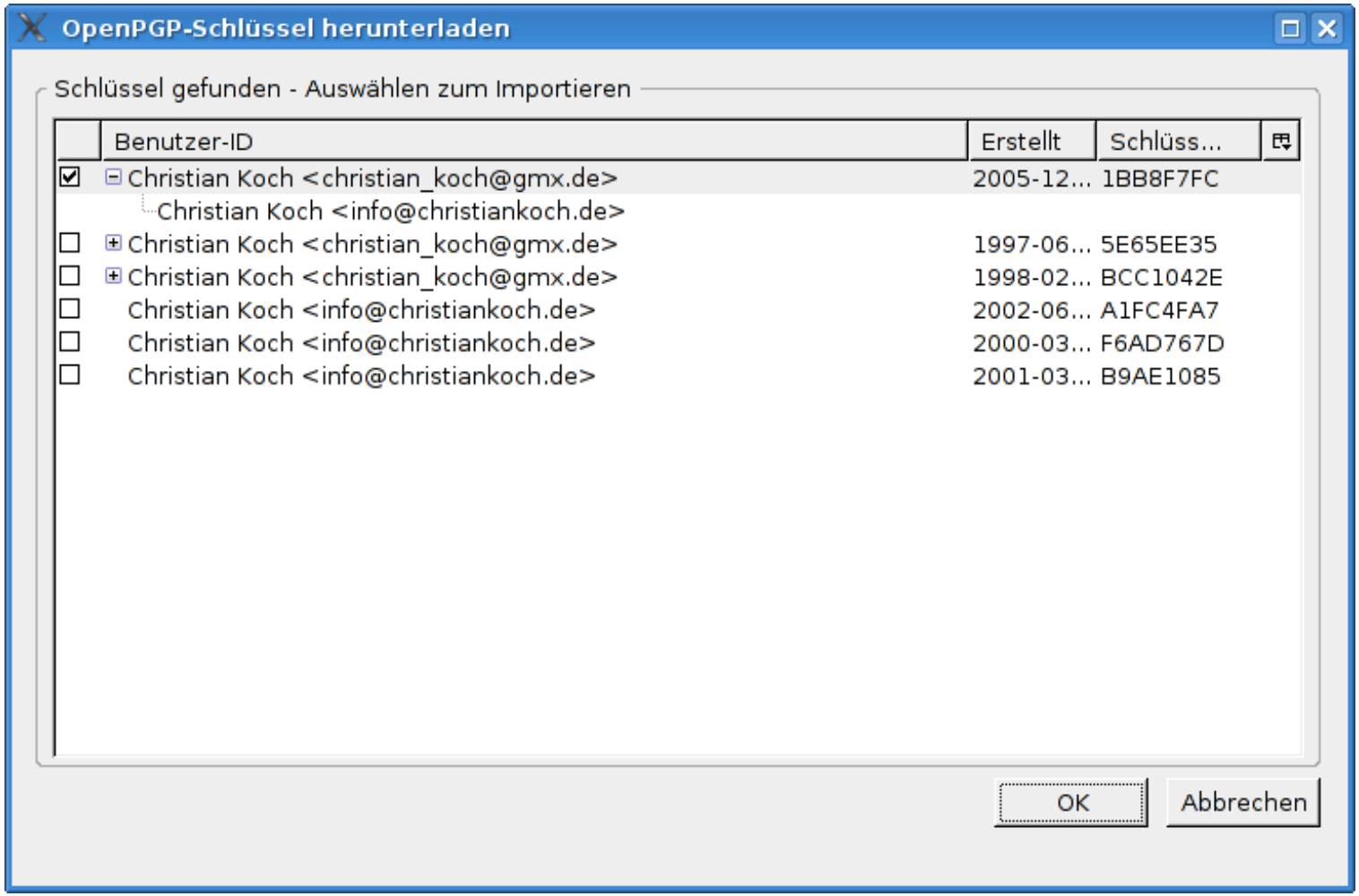
Schlüsseleigenschaften des erzeugten Schlüsselpaares



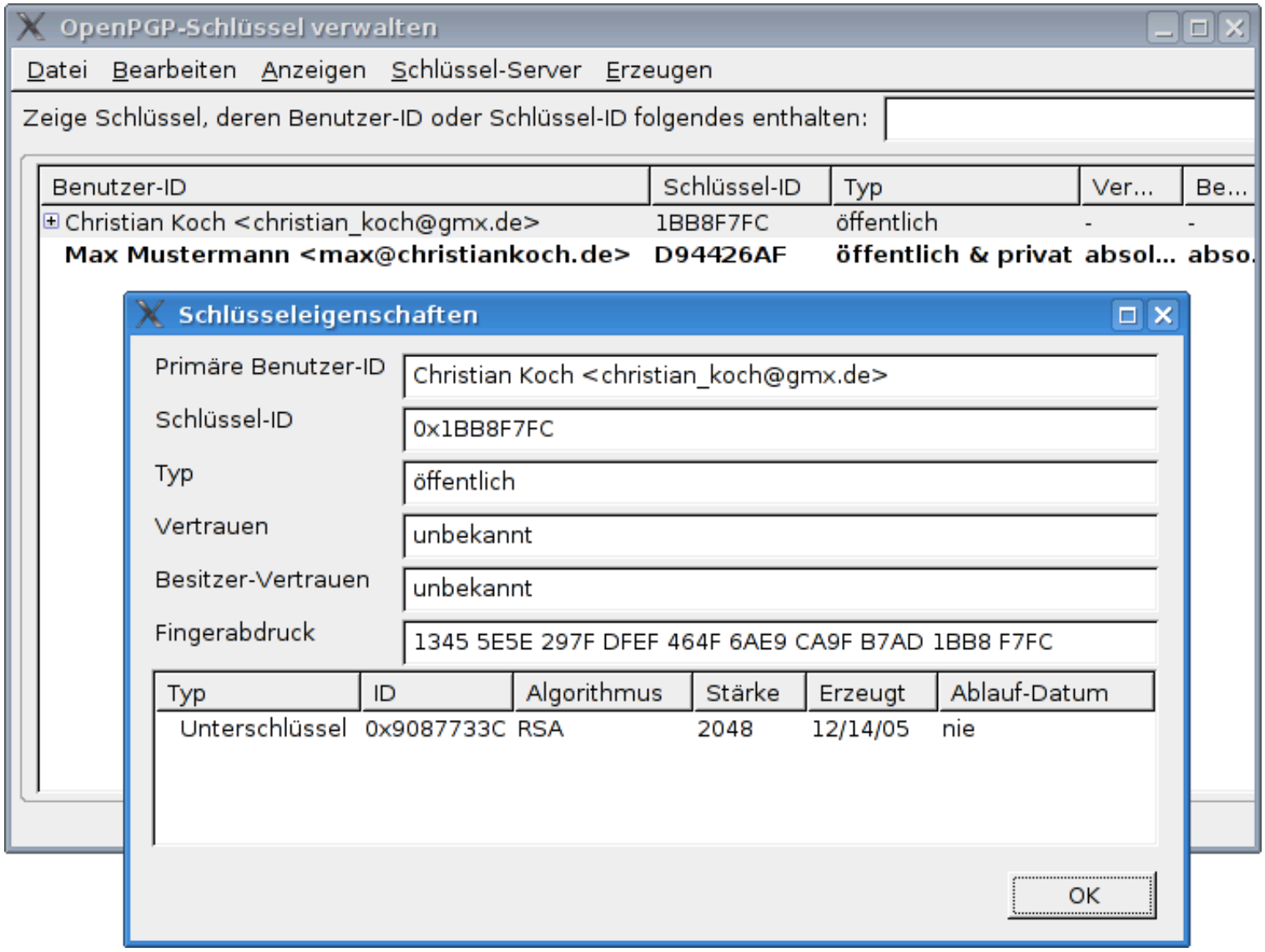
Import eines öffentlichen Schlüssels vom Keyserver (1/2)



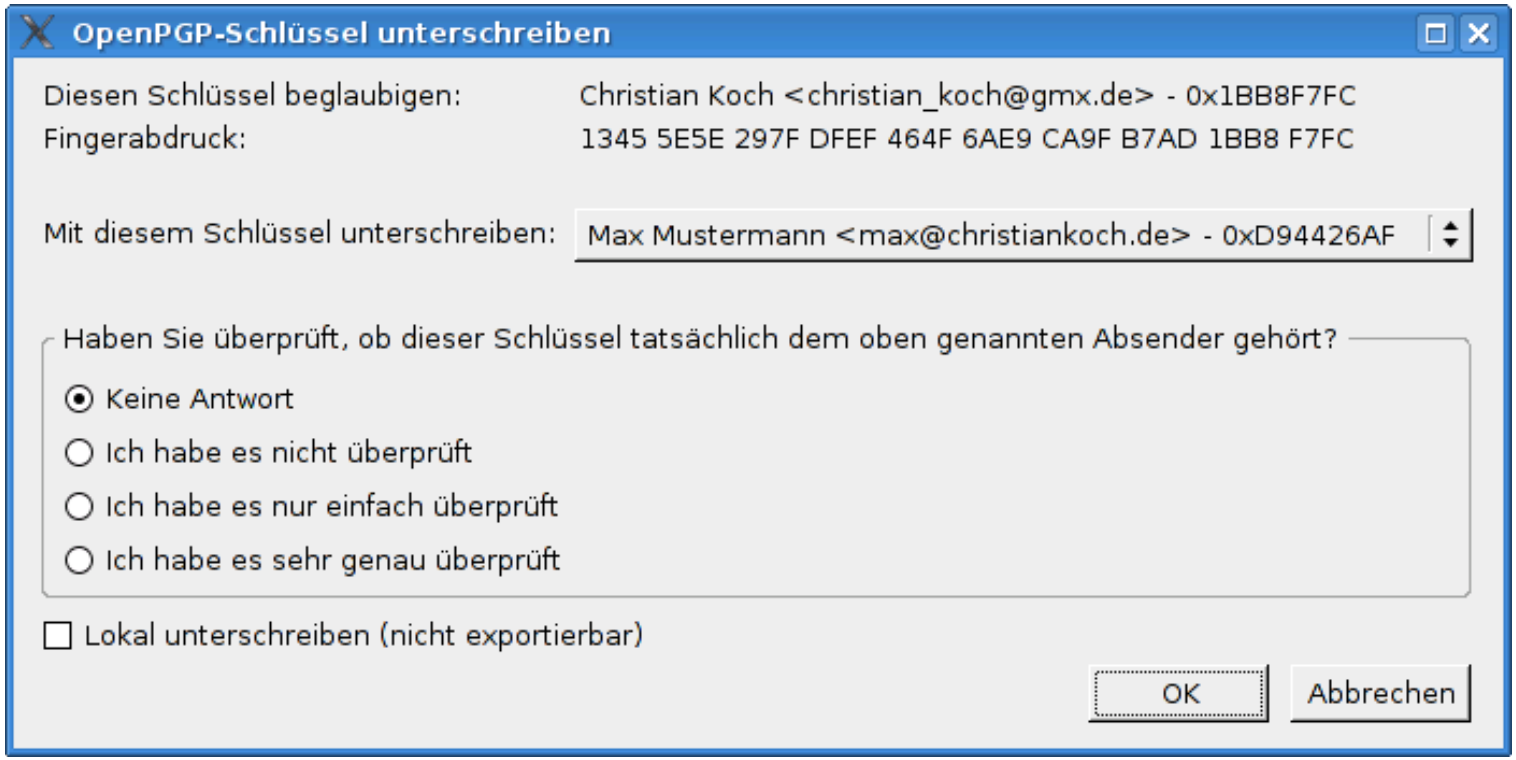
Import eines öffentlichen Schlüssels vom Keyserver (2/2)



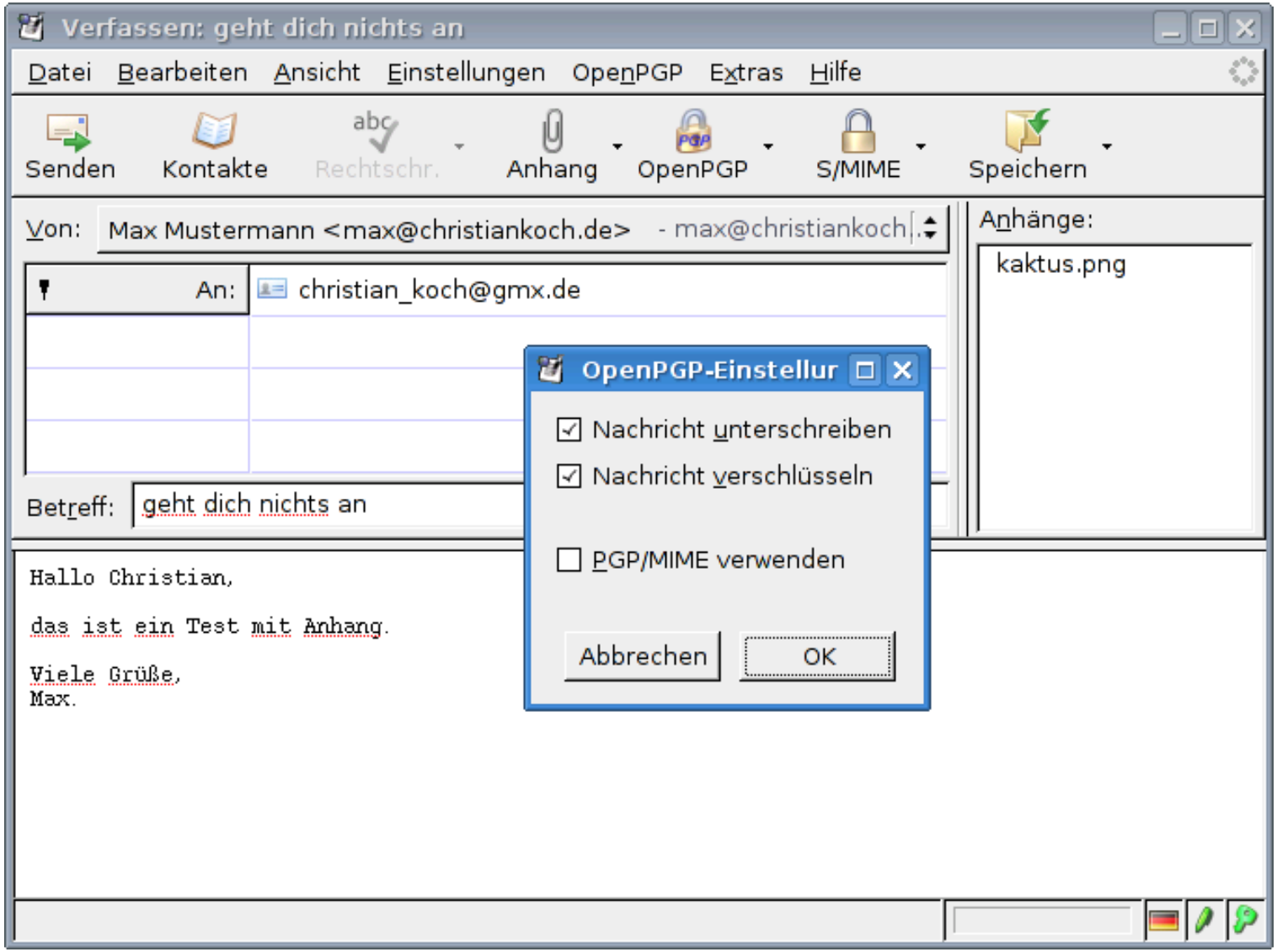
Schlüsseleigenschaften eines unbeglaubigten Schlüssels



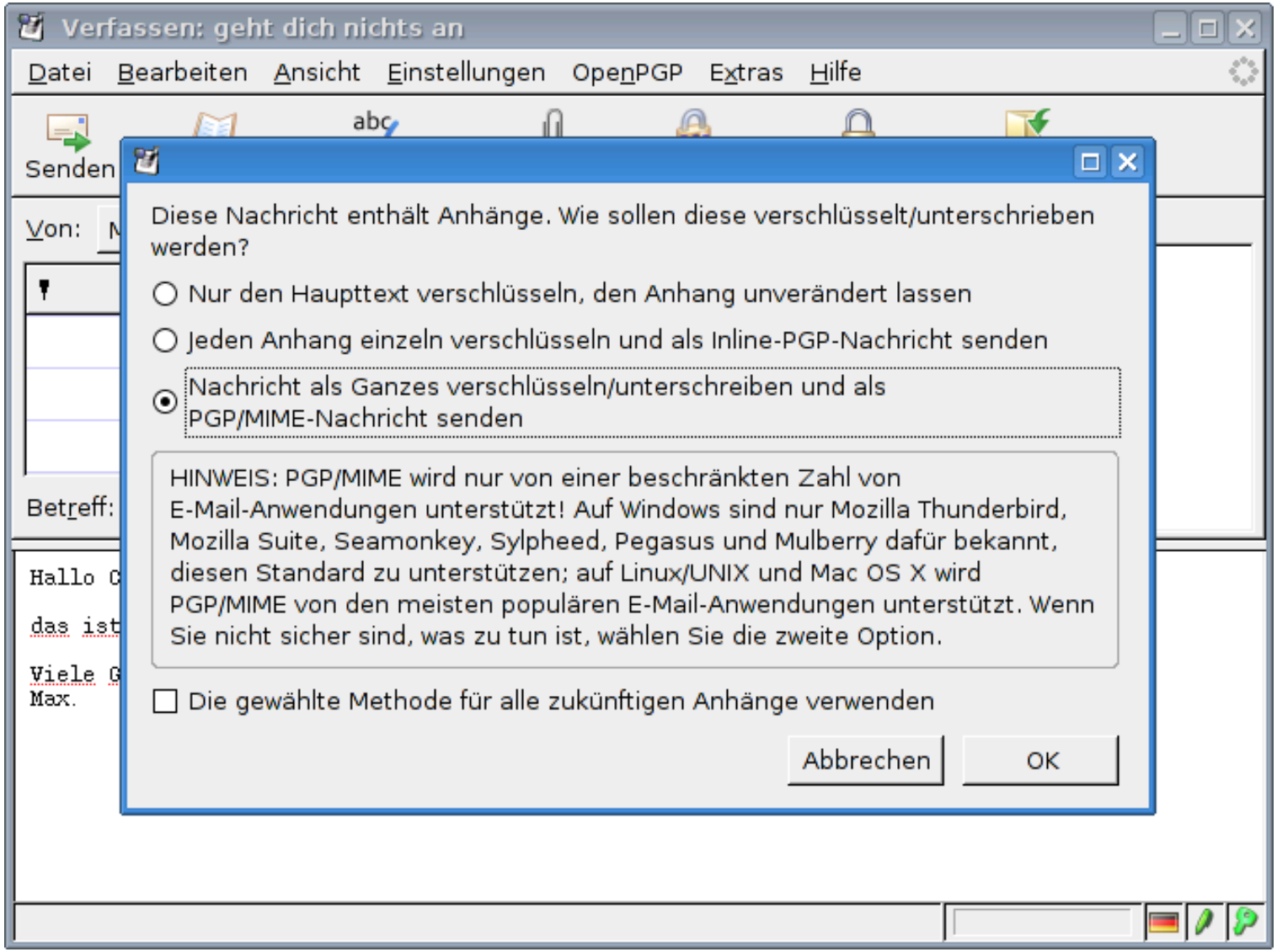
Beglaubigen eines Schlüssels



Verfassen einer verschlüsselten, signierten Nachricht (1/2)

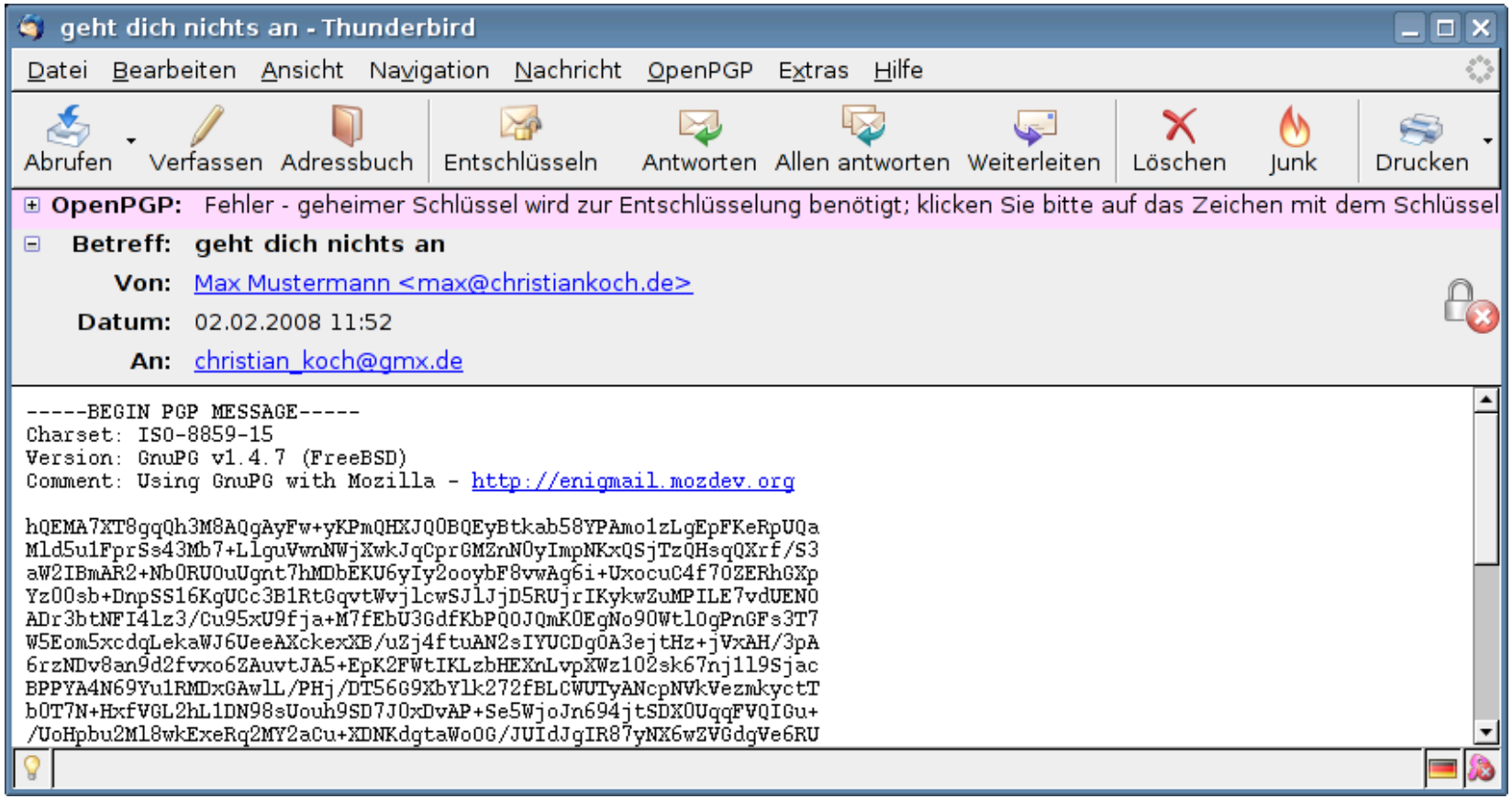


Verfassen einer verschlüsselten, signierten Nachricht (2/2)



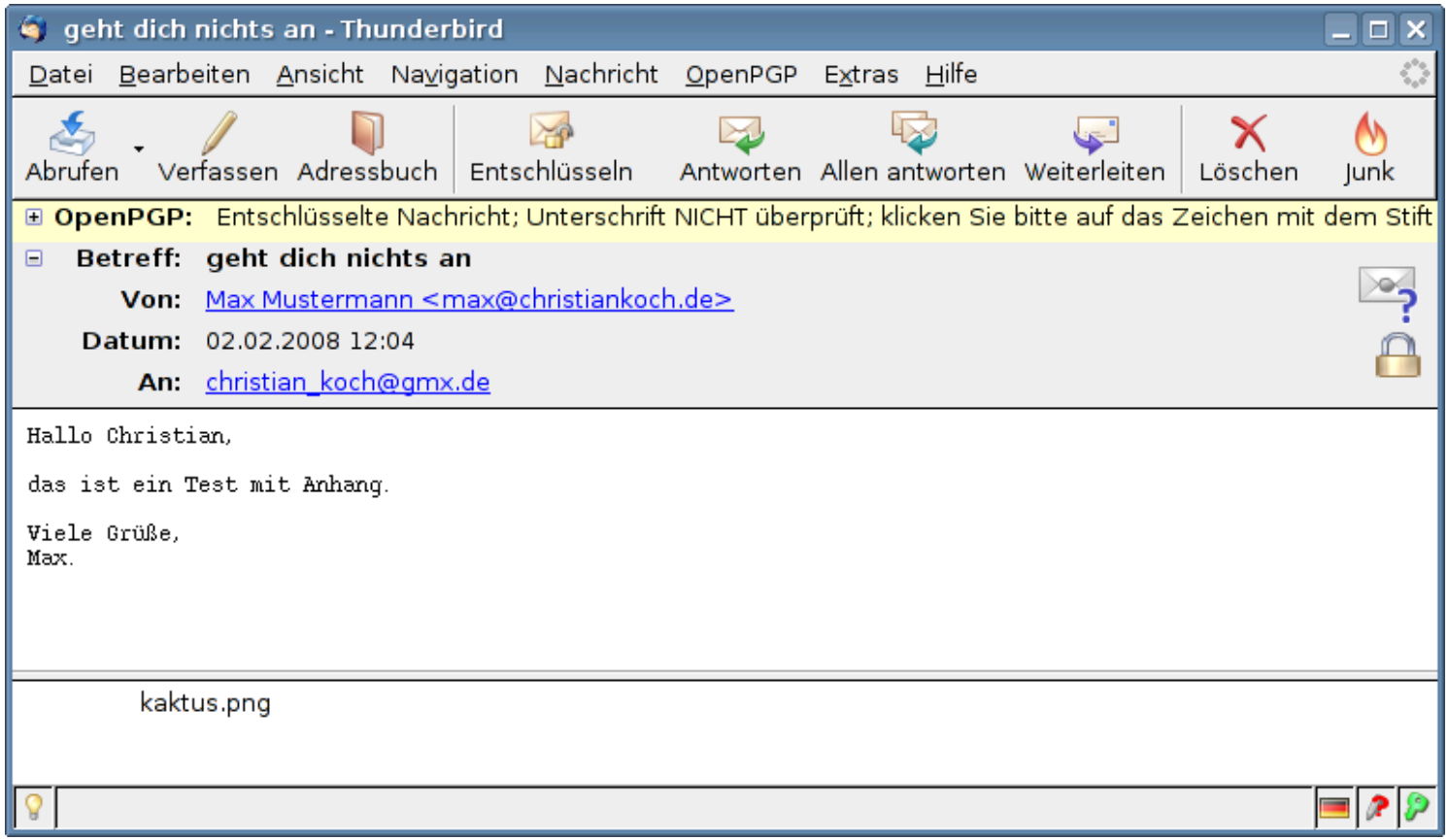
Anzeige einer nicht entschlüsselten Nachricht

Kein passender Empfängerschlüssel, Betreffzeile wird nicht verschlüsselt!



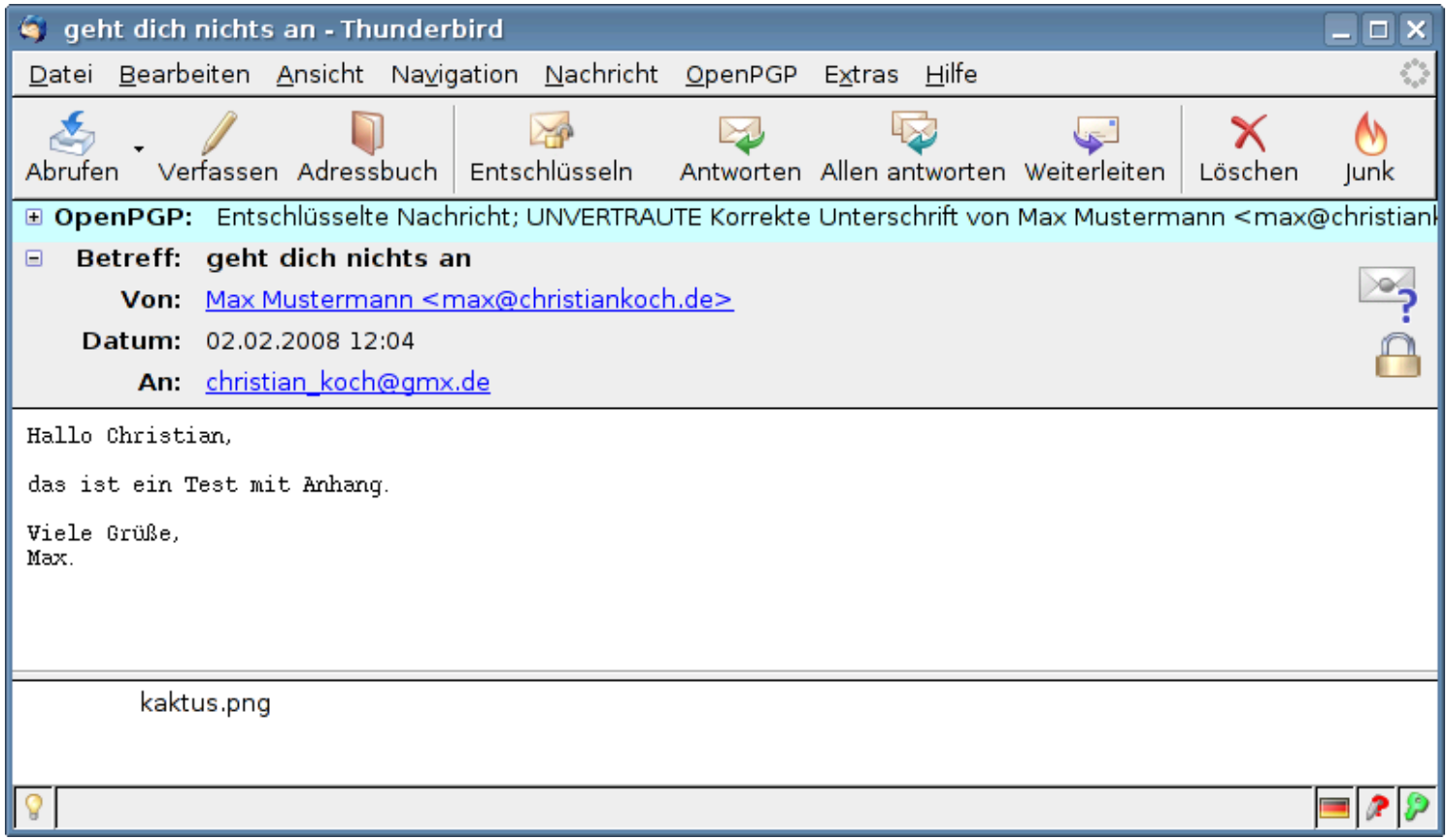
Anzeigen einer entschlüsselten, signierten Nachricht (1/3)

Absenderschlüssel fehlt

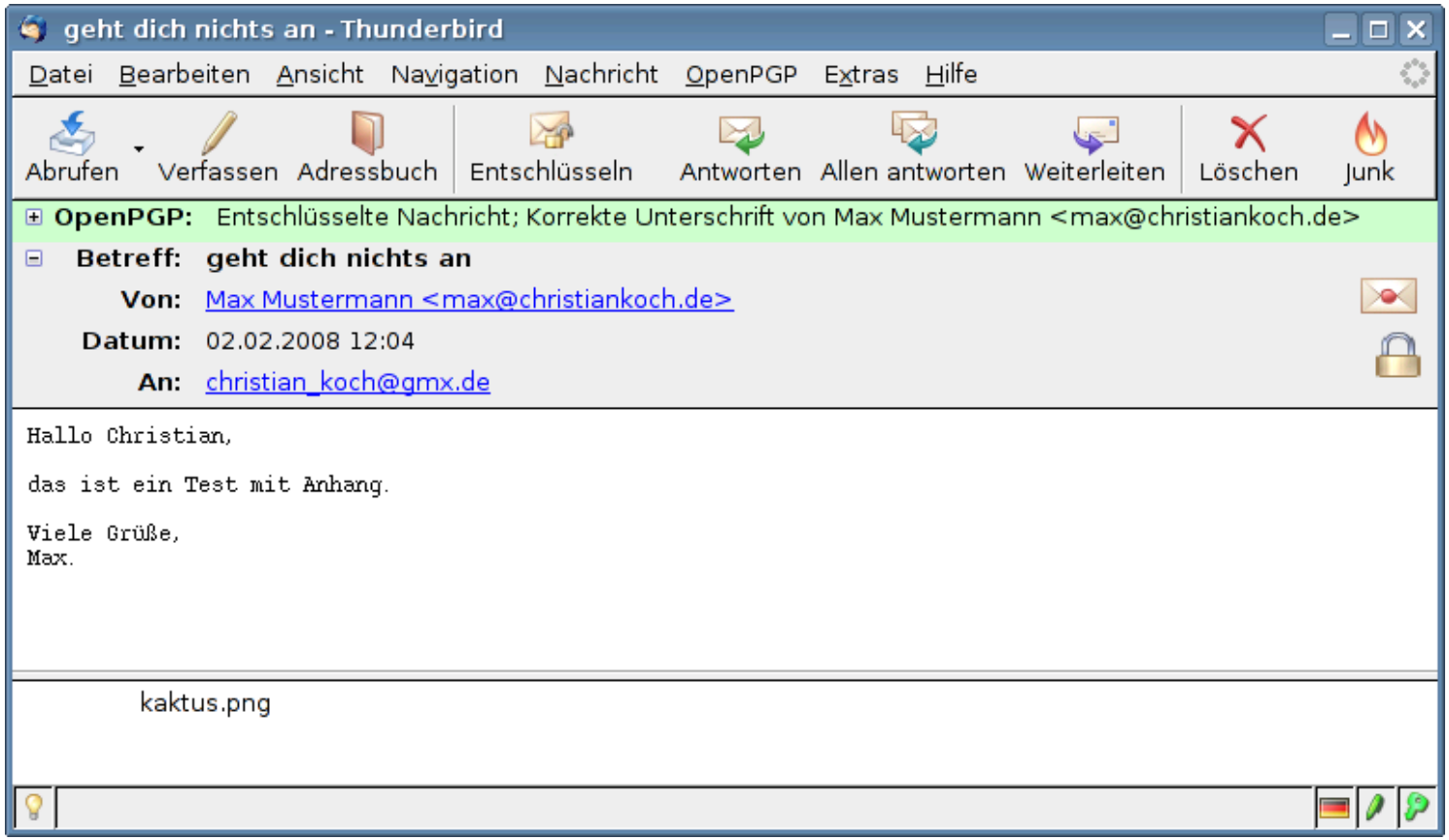


Anzeigen einer entschlüsselten, signierten Nachricht (2/3)

Absenderschlüssel nicht signiert → kein Vertrauen

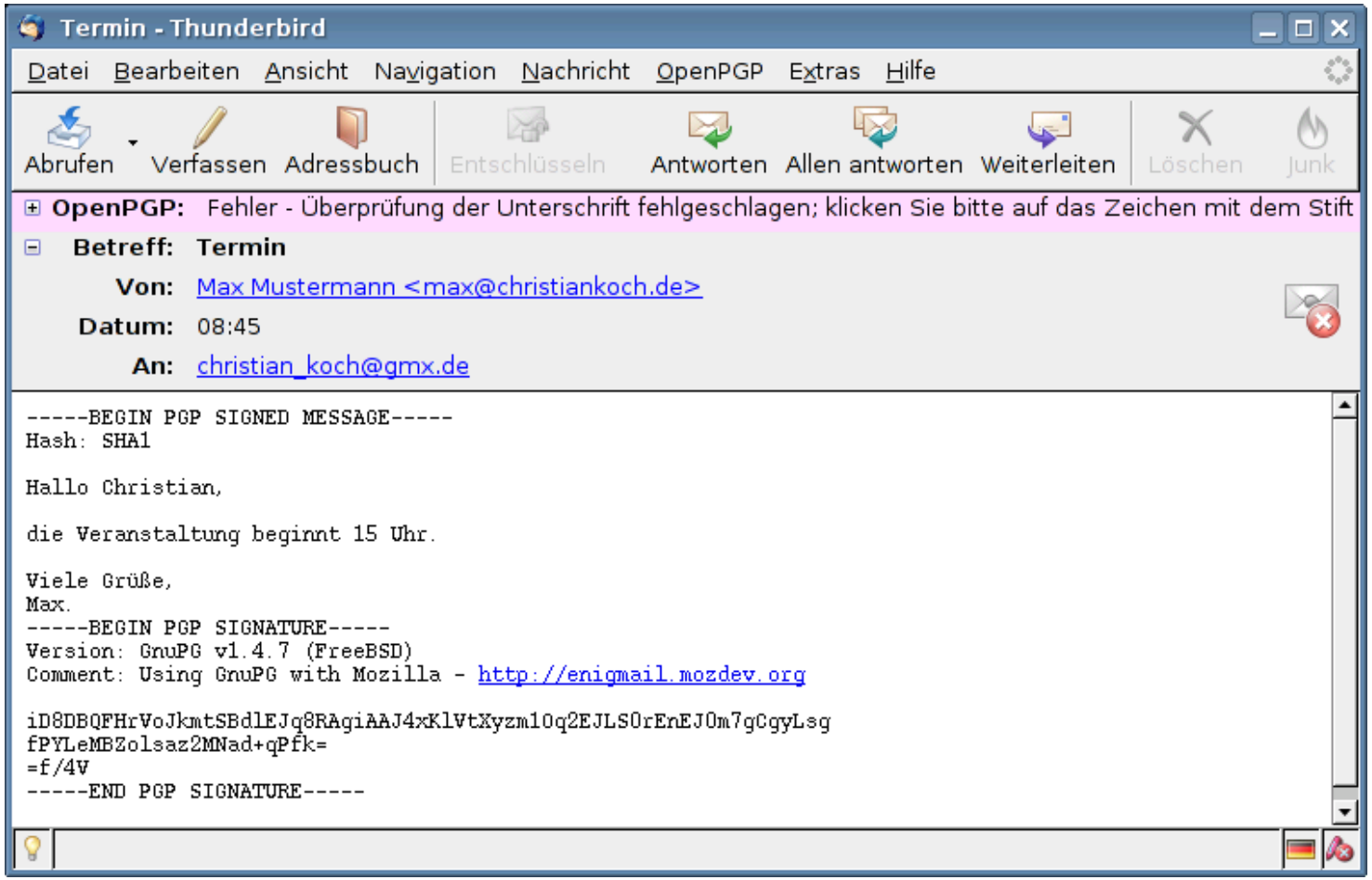


Anzeigen einer entschlüsselten, signierten Nachricht (3/3)



Anzeigen einer signierten, gefälschten Nachricht

Nachrichtentext wurde nach Signierung geändert



Schlußbemerkungen

- realistische Schlüsselgrößen benutzen: Niemand baut eine Tresortür als Wohnungstür ein!
- privaten Schlüssel und Widerrufszertifikat sicher speichern
- privaten Schlüssel in einer geschützten Umgebung verwenden (eigener Computer, ggf. Chipkarte), siehe „Bundestrojaner“
- Sicherheitslücken durch Updates regelmäßig schließen
- keine individualisierte Links in E-Mails anklicken, ggf. anonym surfen[3]
- Verbindungsdaten auch durch Verschlüsselung weiterhin erkennbar, siehe Vorratsdatenspeicherung, ggf. Mixmaster-Remailer benutzen

[3] z. B. `http://tor.eff.org/`

Lizenz