

Verschlüsselung des E-Mail-Verkehrs mit GnuPG

Christian Koch Eric Goller

Chaostreff Leipzig

7. Juni 2008

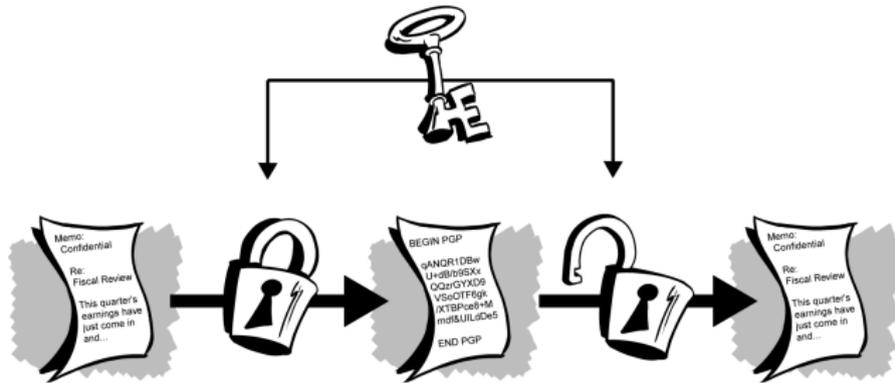
Agenda

- 1 Grundlagen
- 2 GNUPG
- 3 ENIGMAIL
- 4 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
- aktuelle Entscheidung StB 34/07 des BGH: Verschlüsselung von E-Mails begründet keinen dringenden Tatverdacht

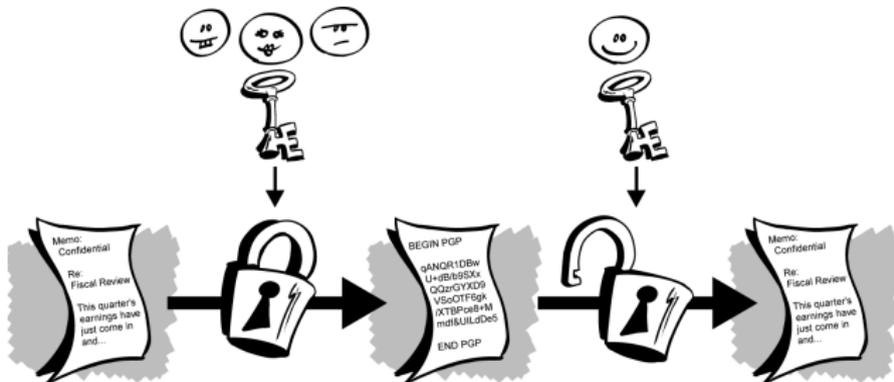
Prinzip der symmetrischen Chiffrierung



© 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 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-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/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 Keyservern², die sich untereinander synchronisieren

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

```
Version: GnuPG v2.0.3 (FreeBSD)
```

```
mQELBEOgWmcBCAD01Qh3ik7sNjSQ1mr+xgLF8FOEwE8e12F03gtYjoCQTvu/3l6H
jAbMGJ638eqwYrpRTfz8CDxIMwWOC2Vk51BLNwew1z+2ec6fmMkZ1ElxWIDp51qF
[...]
```

```
lwN5JTLszmkp6twGMQoennrVfKbKXIpTnd6k8SBw60A1yR4w0KOWMrWma5KIwYEp
iF0jkJEkpmreqc8PO6w83QBHNBpySXfLVJUz8A==
=6RT9
```

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

²z. B. <http://wwwkeys.de.pgpg.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
```

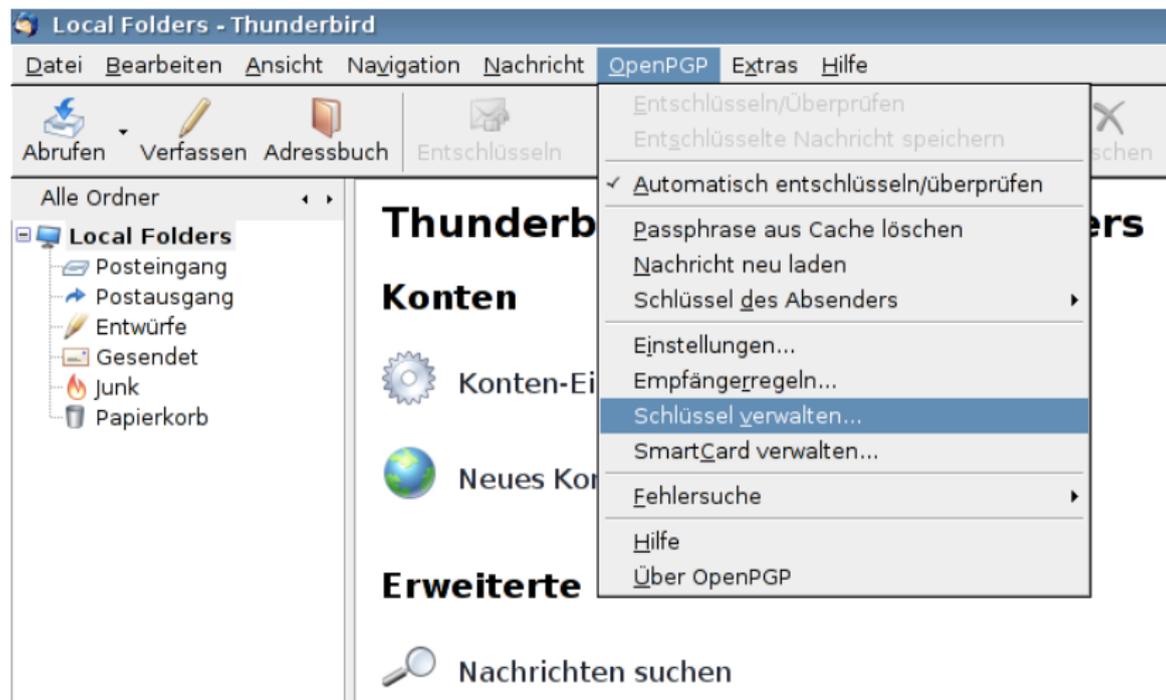
- Schlüssel wird gültig durch ...

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

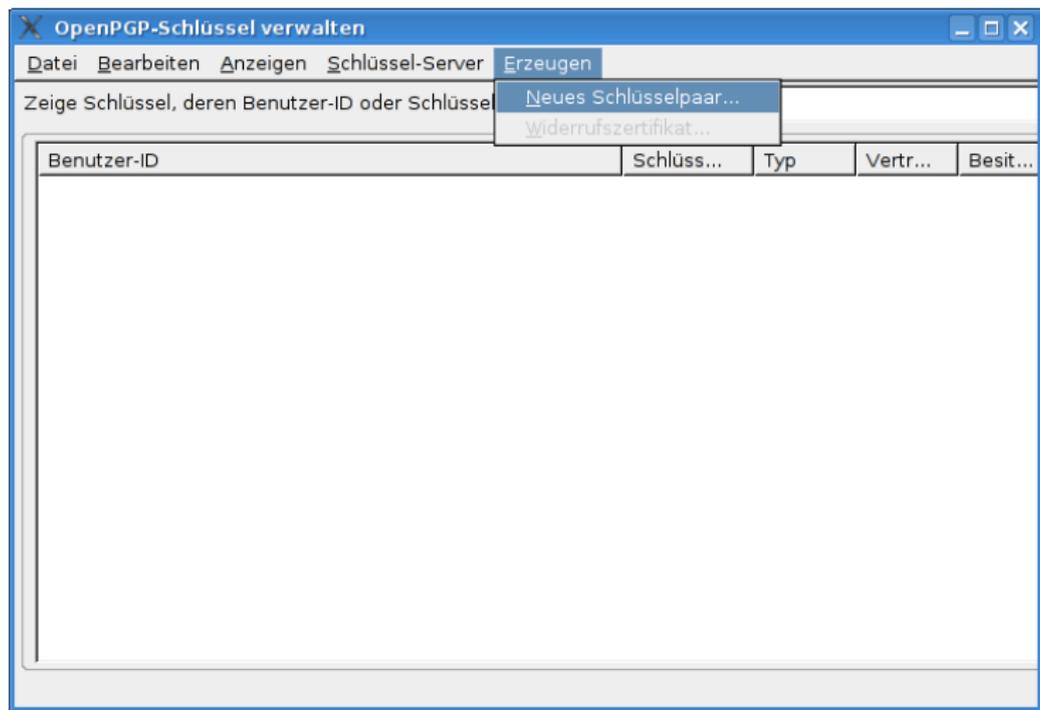
Was ist ENIGMAIL?

- 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)

OpenPGP-Schlüssel erzeugen

Benutzer-ID

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase Passphrase wiederholen

Kommentar

Ablauf-Datum

Schlüssel läuft ab in Jahren Schlüssel läuft nie ab

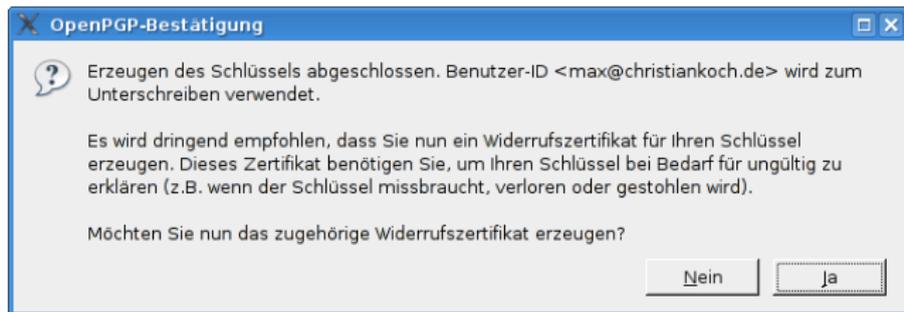
Konsole zum Erzeugen eines Schlüssels

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
- 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.

Schlüsseigenschaften des erzeugten Schlüsselpaars

OpenPGP-Schlüssel verwalten

Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen

Zeige Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten:

Benutzer-ID	Schlüssel-ID	Typ	Ver...	Be...
Max Mustermann <max@christiankoch.de>	D94426AF	öffentlich & privat	absol...	abso...

Schlüsseigenschaften

Primäre Benutzer-ID: Max Mustermann <max@christiankoch.de>

Schlüssel-ID: 0xD94426AF

Typ: Schlüsselpaar

Vertrauen: absolutes Vertrauen

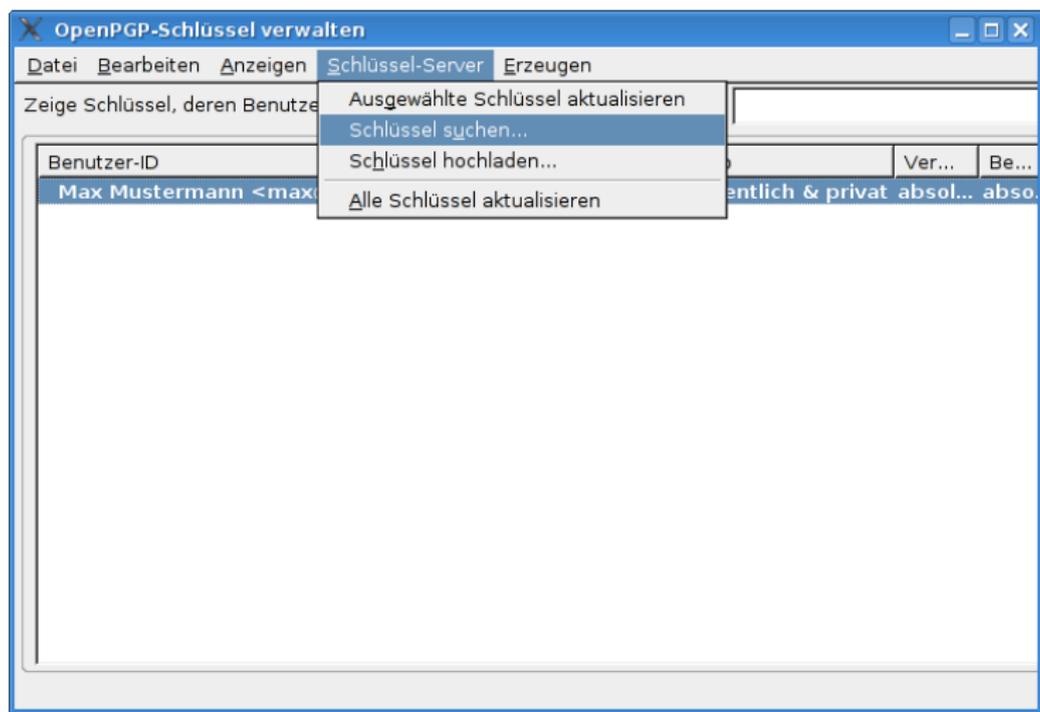
Besitzer-Vertrauen: absolutes Vertrauen

Fingerabdruck: 560C 2166 A0A7 4F92 01B7 530F 926B 5205 D944 26AF

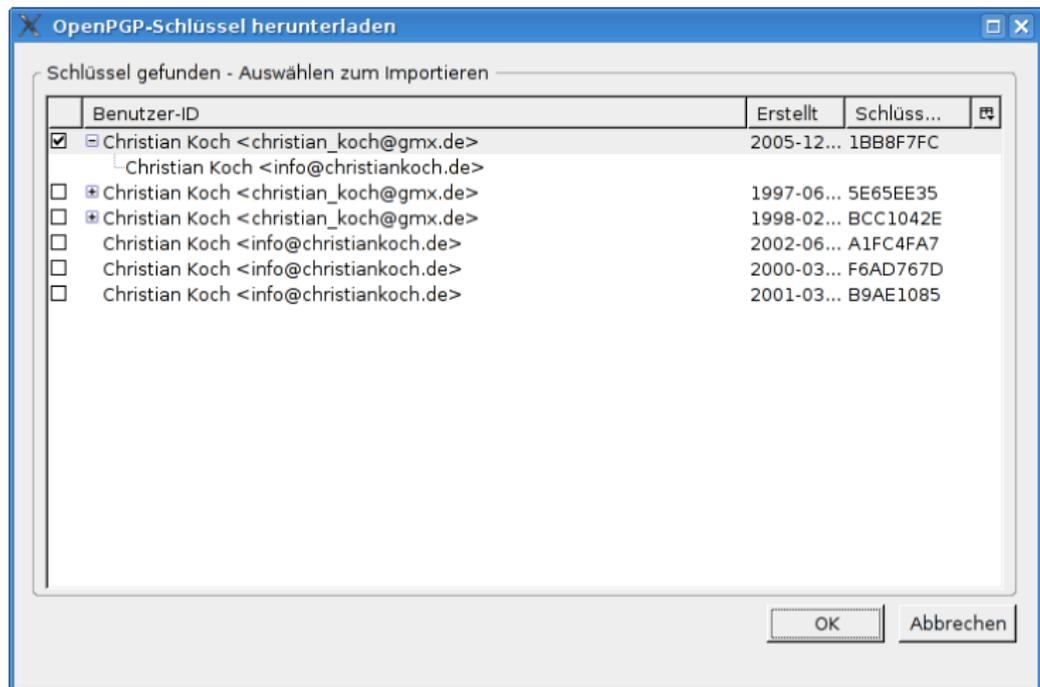
Typ	ID	Algorithmus	Stärke	Erzeugt	Ablauf-Datum
Unterschlüssel	0x1F3FA357	ELG	2048	02/02/08	01/31/13

OK

Import eines öffentlichen Schlüssels vom Keyserver (1/2)



Import eines öffentlichen Schlüssels vom Keyserver (2/2)



Schlüsseigenschaften eines unbeglaubigten Schlüssels

OpenPGP-Schlüssel verwalten

Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen

Zeige Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten:

Benutzer-ID	Schlüssel-ID	Typ	Ver...	Be...
Christian Koch <christian_koch@gmx.de>	1BB8F7FC	öffentlich	-	-
Max Mustermann <max@christiankoch.de>	D94426AF	öffentlich & privat absol...	absol...	absol...

Schlüsseigenschaften

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

Schlüssel-ID: 0x1BB8F7FC

Typ: öffentlich

Vertrauen: unbekannt

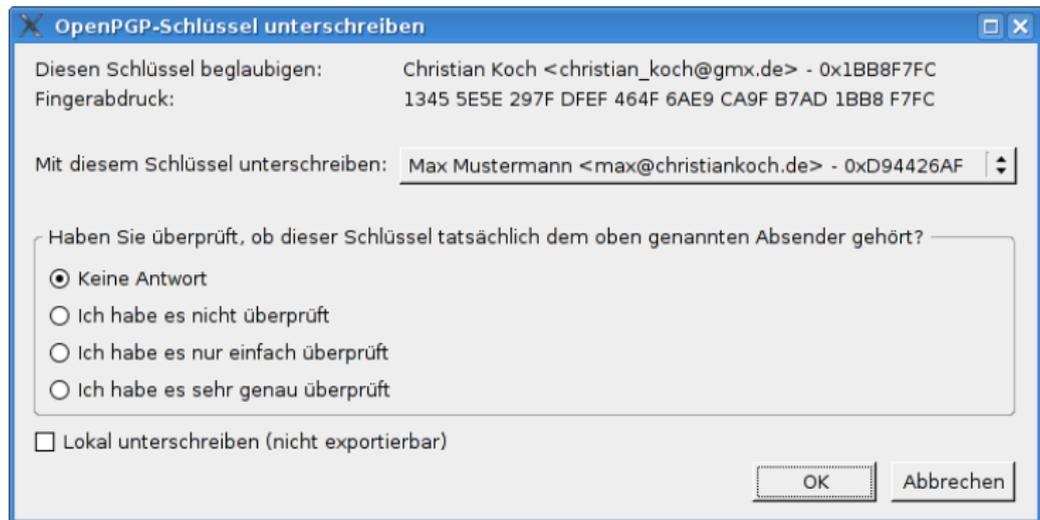
Besitzer-Vertrauen: unbekannt

Fingerabdruck: 1345 5E5E 297F DFEF 464F 6AE9 CA9F B7AD 1BB8 F7FC

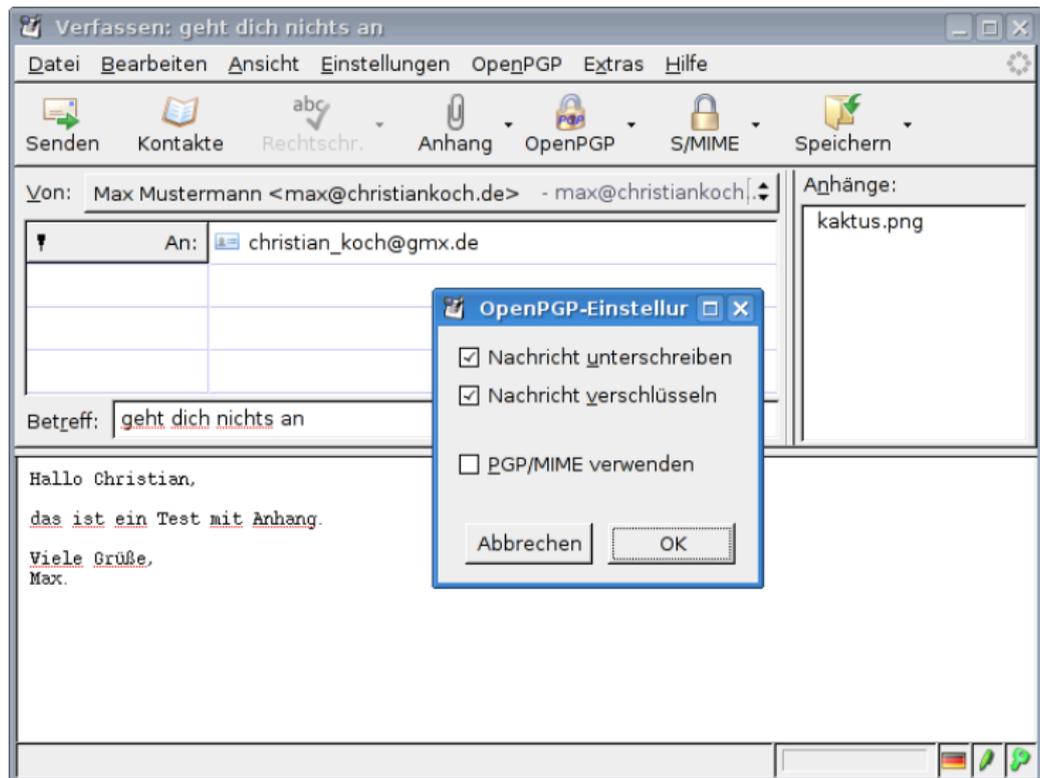
Typ	ID	Algorithmus	Stärke	Erzeugt	Ablauf-Datum
Unterschlüssel	0x9087733C	RSA	2048	12/14/05	nie

OK

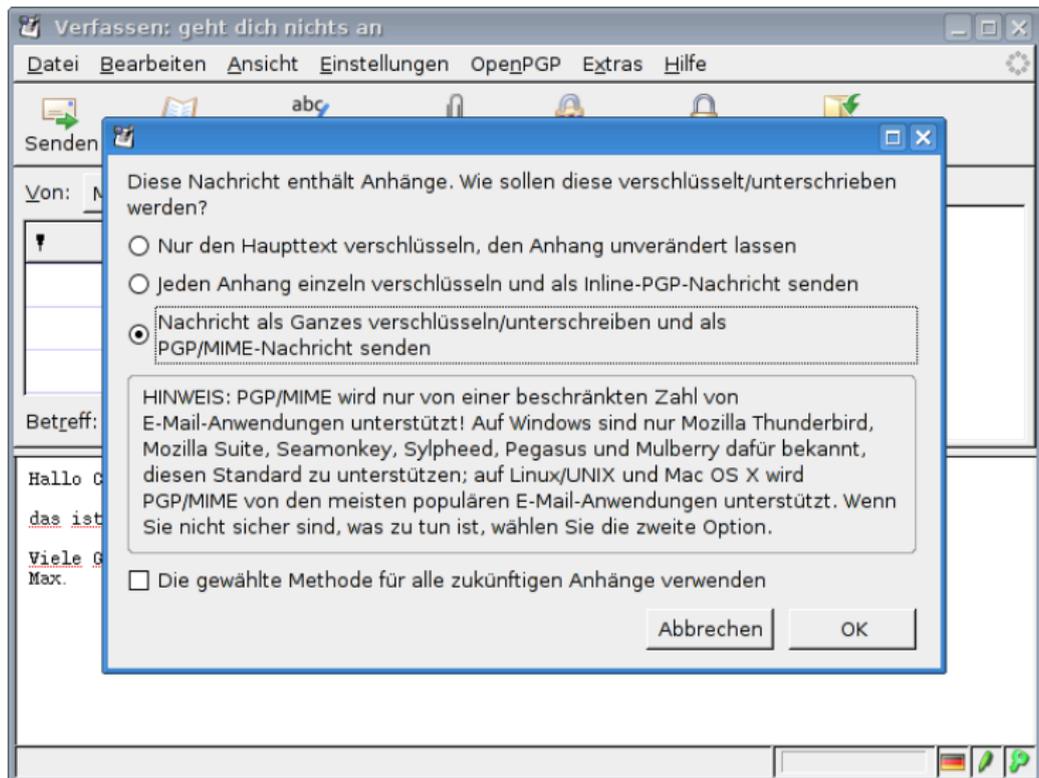
Beglaubigen eines Schlüssels



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!

geht dich nichts an - Thunderbird

Datei Bearbeiten Ansicht Navigation Nachricht OpenPGP Extras Hilfe

Abrufen Verfassen Adressbuch Entschlüsseln Antworten Allen antworten Weiterleiten Löschen Junk Drucken

OpenPGP: Fehler - geheimer Schlüssel wird zur Entschlüsselung benötigt; klicken Sie bitte auf das Zeichen mit dem Schlüssel

Betreff: geht dich nichts an

Von: Max Mustermann <max@christiankoch.de>

Datum: 02.02.2008 11:52

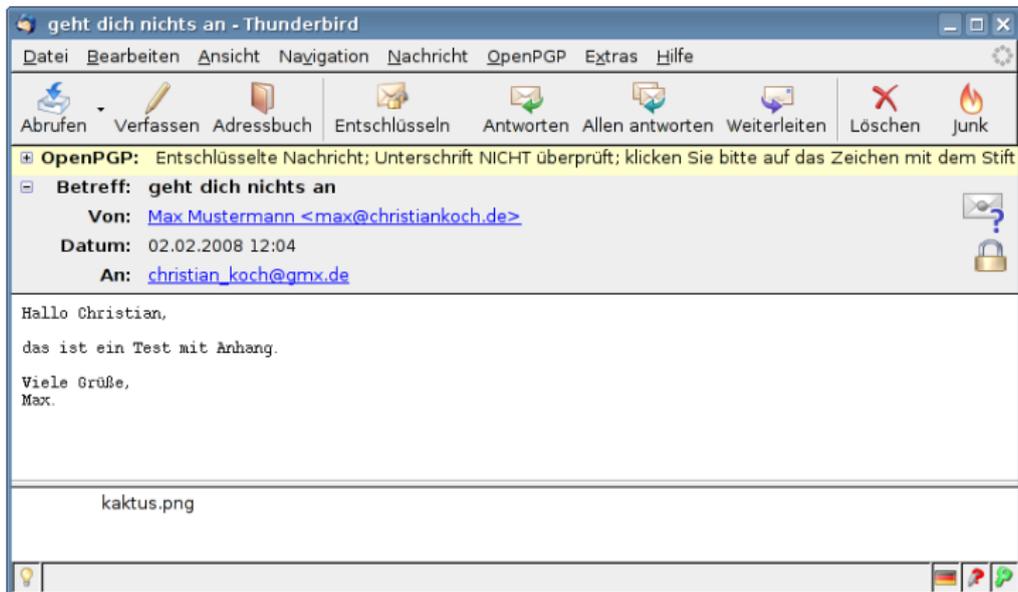
An: christian_koch@gmx.de

-----BEGIN PGP MESSAGE-----
 Charset: ISO-8859-15
 Version: GnuPG v1.4.7 (FreeBSD)
 Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

hQEMATXT8gqQh3M8A0qAyFw+yKPm0HXJ00B0EyBtkab58YPAmo1zLgEpFkeRpU0a
 M1d5ulFprSs43Mb7+LlguVwnWnjXvkJqCprGMZnN0yImpNKxQSjTz0HsqQXrf/S3
 aW2IBnAR2+Nb0RU0uUgnt7hMDbEKU6yIy2ooybF8vwAg6i+UxocuC4f70ZERhGnq
 Yz00sb+DnpSS16KgUCc3B1Rt6qvtWvjLcwSJLjD5RUjrIKykwZuMPiLE7vdUENO
 AD: 3btNF14lz3/Cu95xU9fja+M7fEBu3GdFKbP0JQmK0EGNo90WtL0qPnGFs3T7
 W5Eom5xcdqLekawJ6UeeAKckexXB/uZj4ftuAN2sIYUCDg0A3ejtHz+jVxAH/3pA
 6rzNDv8an9d2fvxo6ZAvvtJA5+EpK2FwtIKLzbHEXrLvpXWz102sk67nj119Sjac
 BPPYA4n69YulRMDxGAWLL/PHj/DT5669XbYlK272fBLCWUtyANcpNwVezmkycT
 b0T7N+HxfV6L2hL1DM98sUouh9SD7J0uVAP+Se5Wjo3n694jtsDXU0uqqPVQ16u+
 /UoHpbn2M18wkExeRq2MY2aCu+XDNKdgtawo0G/JUIDjgIR87yNX6wZV6dgVe6RU

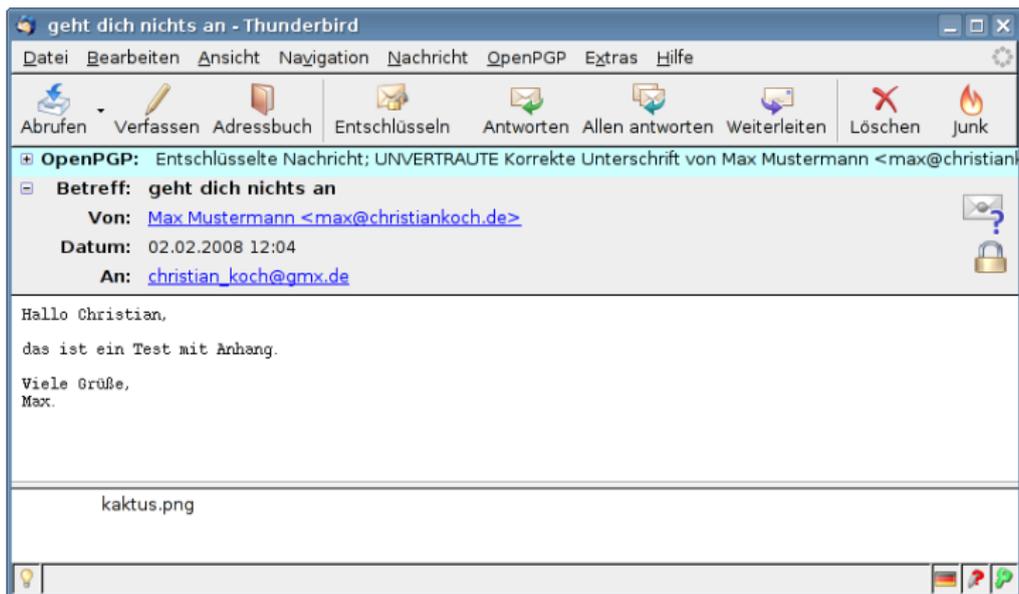
Anzeigen einer entschlüsselten, signierten Nachricht (1/3)

Absenderschlüssel fehlt

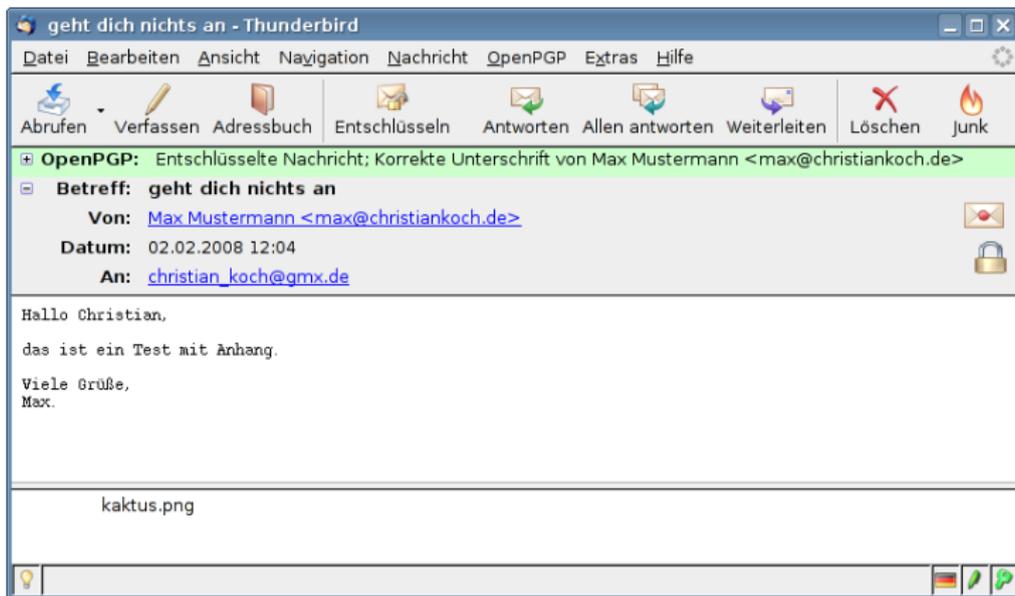


Anzeigen einer entschlüsselten, signierten Nachricht (2/3)

Absenderschlüssel nicht signiert → kein Vertrauen

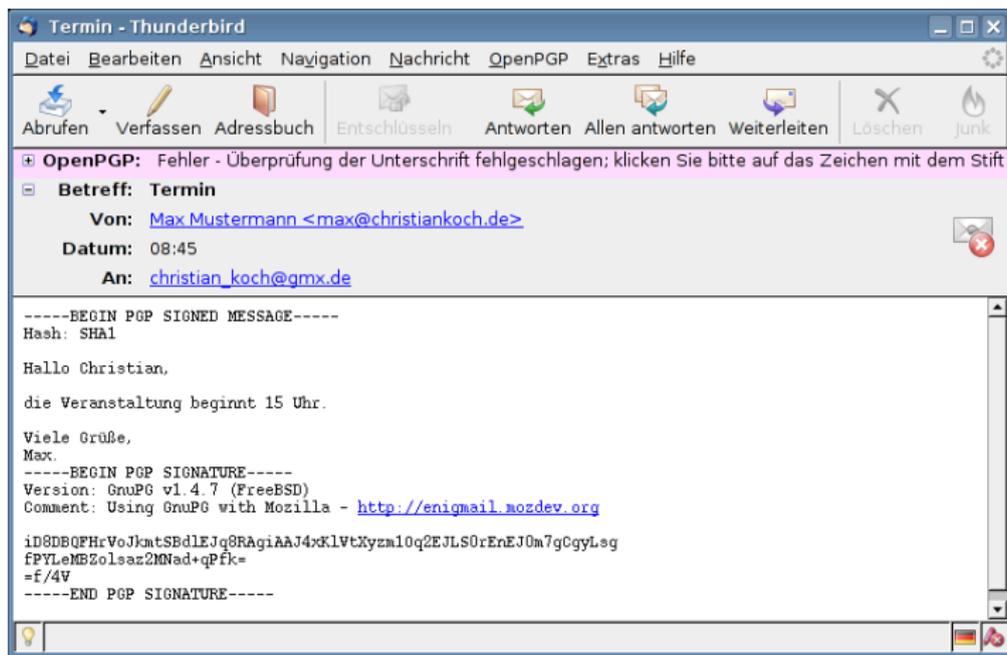


Anzeigen einer entschlüsselten, signierten Nachricht (3/3)



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 surfen³
- Verbindungsdaten auch durch Verschlüsselung weiterhin erkennbar, siehe Vorratsdatenspeicherung, ggf. Mixmaster-Remailer benutzen

³z. B. <http://tor.eff.org/>



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.