

Verschlüsselung des E-Mail-Verkehrs mit GnuPG

Christian Koch

`christian_koch@gmx.de`

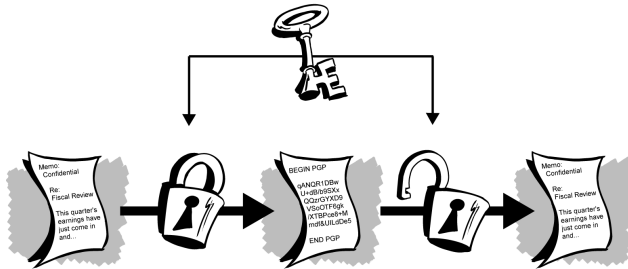
5. Mai 2007

- 1 Grundlagen
- 2 GnuPG
- 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

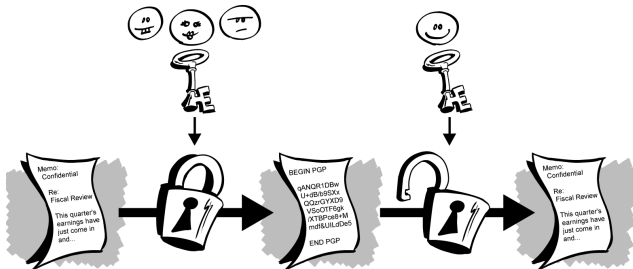
Prinzip der symmetrischen Chiffrierung



© PGP Corporation.

Analogie: 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)
```

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

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

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

²z. B. <http://wwwkeys.de.pgp.net/>

Authentizität fremder Schlüssel

- Ist ein vom Keyserver gelieferter Schlüssel authentisch?

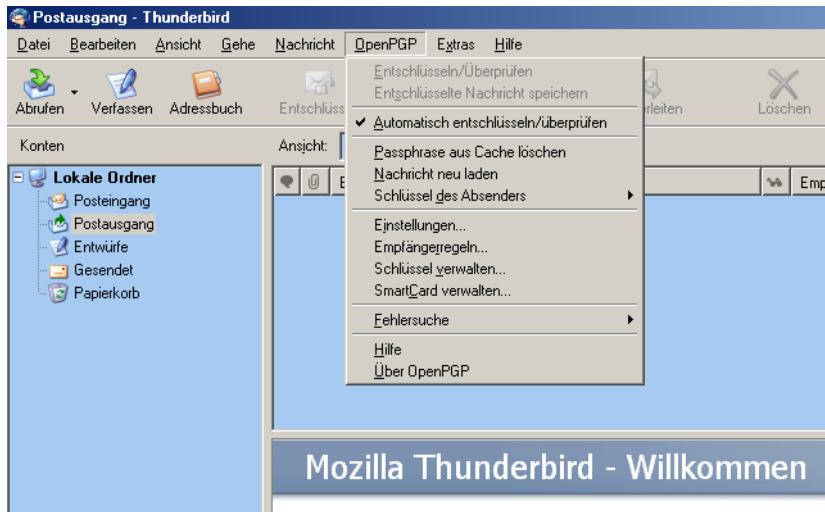
```
Type bits/keyID      Date           User ID
pub  2048R/1BB8F7FC  2005-12-14  Christian Koch <christian_koch@gmx.de>
                                Christian Koch <info@christiankoch.de>
Fingerprint=1345 5E5E 297F DFEF 464F 6AE9 CA9F B7AD 1BB8 F7FC
```

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

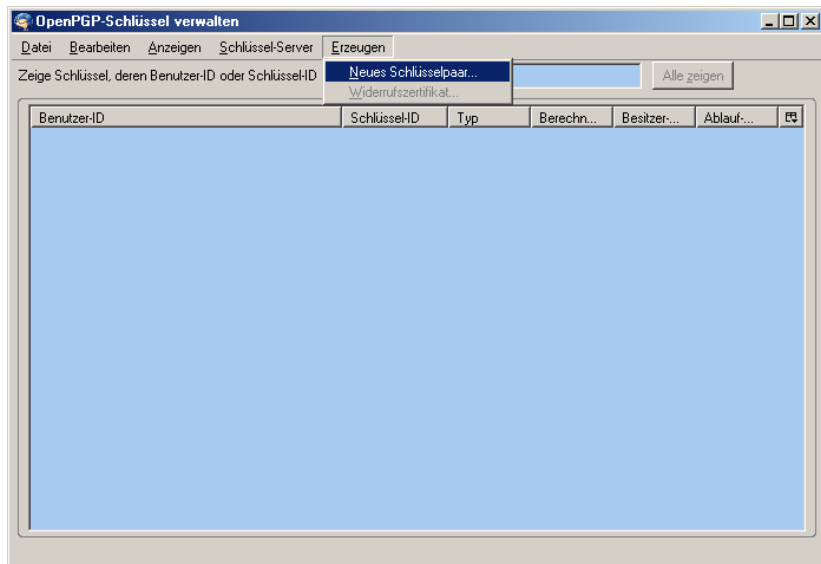
Was ist ENIGMAIL?

- 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



Schlüsselverwaltung



Schlüsselpaar erzeugen (1/2)

OpenPGP-Schlüssel erzeugen [X]

Benutzer-ID [v]

Schlüssel zum Unterschreiben verwenden

keine Passphrase

Passphrase Passphrase wiederholen

Kommentar

Ablauf-Datum

Schlüssel läuft ab in [v] Schlüssel läuft nie ab

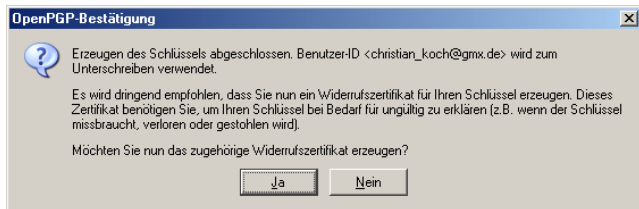
Konsole zum Erzeugen eines Schlüssels

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.

Schlüsseigenschaften des erzeugten Schlüsselpaares

OpenPGP-Schlüssel verwalten

Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen

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

Benutzer-ID	Schlüssel-ID	Typ	Berechn...	Besitzer...	Ablauf...	
Christian Koch <christian_koch@gmx.de>	60710B13	öffentlich...	absolutes...	absolutes...	08.05.2007	

Schlüsseigenschaften X

Primäre Benutzer-ID:

Schlüssel-ID:

Typ:

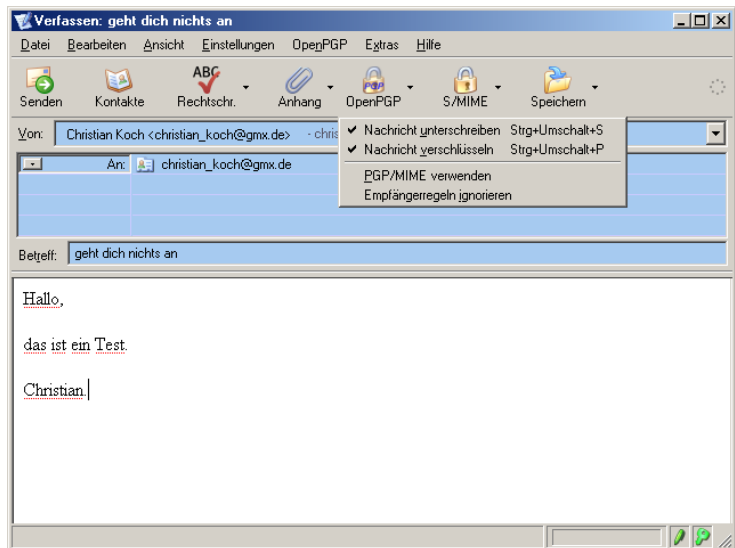
Berechnetes Vertrauen:

Besitzer-Vertrauen:

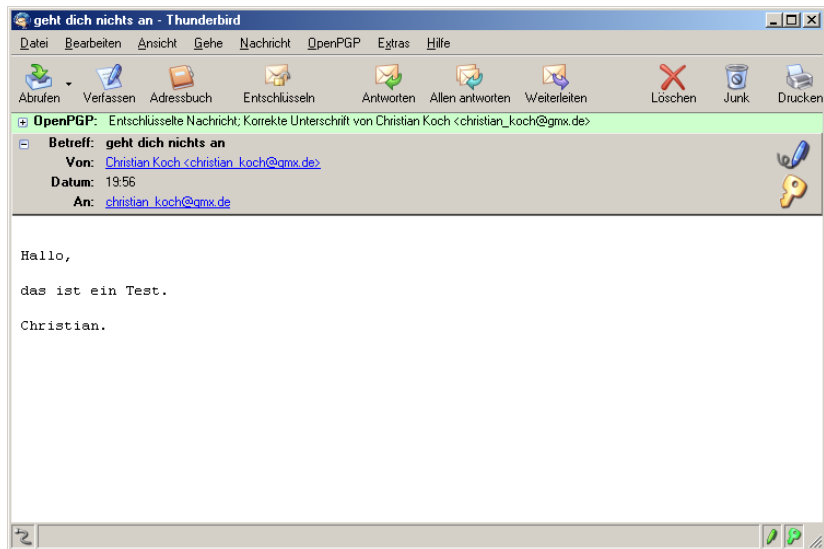
Fingerabdruck:

Typ	ID	Algorit...	S...	Erzeugt	Ablauf-Datum
Untersch...	0x3B87D650	RSA	2048	03.05.2007	08.05.2007

Verfassen einer verschlüsselten Nachricht



Anzeigen einer entschlüsselten Nachricht



Anzeigen einer nicht entschlüsselbaren Nachricht

Achtung: Betreffzeile wird nicht verschlüsselt!

geht dich nichts an - Thunderbird

Datei Bearbeiten Ansicht Gehe Nachricht OpenPGP Extras Hilfe

Abrufen Verlassen Adressbuch Entschlüsseln Antworten Allen antworten Weiterleiten Löschen Junk Drucken

OpenPGP: Fehler - keine Passphrase angegeben

Betreff: geht dich nichts an

Von: Christian Koch <christian_koch@gmx.de>

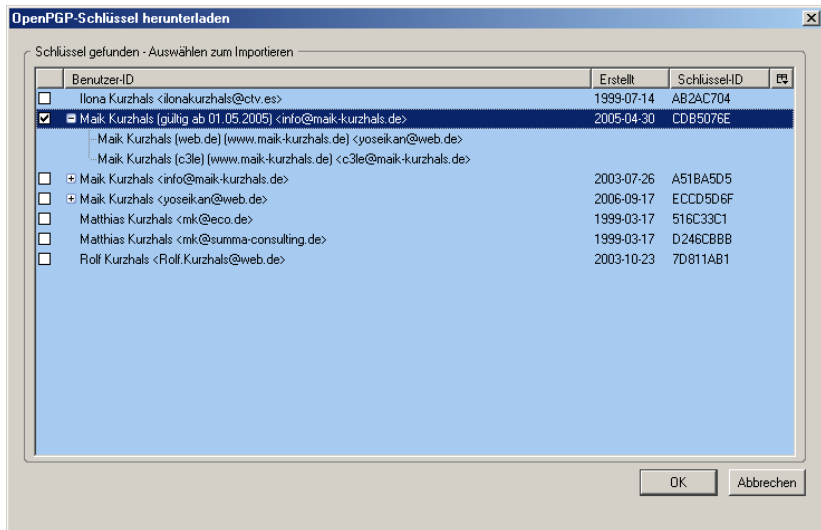
Datum: 19:56

An: christian_koch@gmx.de

-----BEGIN PGP MESSAGE-----
 Charset: ISO-8859-15
 Version: GnuPG v1.4.7 (MingW32)
 Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

hQEEM7rqZfP8et9jAQf/dkCBhIOHZTCD2cGT06FSVqafaiayXbeGAtS455qvEim+Y
 uQskQysi9c1+d8iZM4K2zRo5Z8mjPsgJAgLfEdz4KObg3fa6patqcu7T3Ombd2EK
 +O18VAb/hwZ1SbYWMYPZvDwUokGjFYJQB4ToS78nTJeYOhEoJkWWbQqk8kpP17z
 DkPQwtssPttD1b+55sHY7f4w45RK+NRP1wwU18mnSV1WwCrMAyOdVWO6R+BvGpgo
 OeE9MhmYp0i70/VAr4uUog7nyl6pZatFhdJ2cF9TIowBCbKHXCmnNRbng7kUkh04
 bcPC7FySMoxCOZPtyeUsAmbKuOPMcOP+TS/NI1FQz9LA0AEMenenB/n4HPpvxUxe
 cttGxI3qW19bBqSR83dvnNmjGS2UIzRpGukb3PHUER4E1REdl13VnvHUyof+aXK
 FZhpakDQd5sWaYgk12pY9j8SMZpy19mEKZ6Ah1RetYperf48QK8bzy2Z3o6Rrjd
 yBgd7sp9DZwJbHIPASzvEsIvdHHS57gdrEvFw+rvyZr+xaJcZd6Lcm3dQFOBEZ+z
 UzRtMez6BbAYwraj3MDRR1yJarar5STKeKZBem1JVhd6Sm5y1QP3edWo87+/BSsp
 2uEOOGNBj5ydfHmSSUz6ubWkaJNNjfykBC/+k51Q0GHeqYDKTvgp/Q5I25+d+W
 AqaOulZ3EpxGTzmf2Y4t/7gp8LSq+L1/jgdtRwhMIzntbUCJKALxKWEz+mXFDoV

Import eines Schlüssels vom Keyserver



Schlüsseleigenschaften eines unbeglaubigten Schlüssels

Schlüsseleigenschaften ✕

Primäre Benutzer-ID: Maik Kurzhals (gültig ab 01.05.2005) <info@maik-kurzhals.de>

Schlüssel-ID: 0xCDB5076E

Typ: öffentlich

Berechnetes Vertrauen: unbekannt

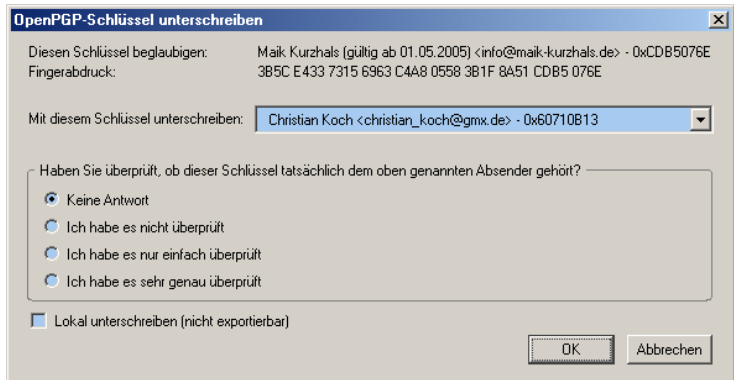
Besitzer-Vertrauen: unbekannt

Fingerabdruck: 3B5C E433 7315 6963 C4A8 0558 3B1F 8A51 CDB5 076E

Typ	ID	Algorit...	S...	Erzeugt	Ablauf-Datum
Untersch...	0x5C6E0097	ELG	2048	30.04.2005	nie

OK

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/>



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.