E-Mail Verschlüsselung mit Enigmail

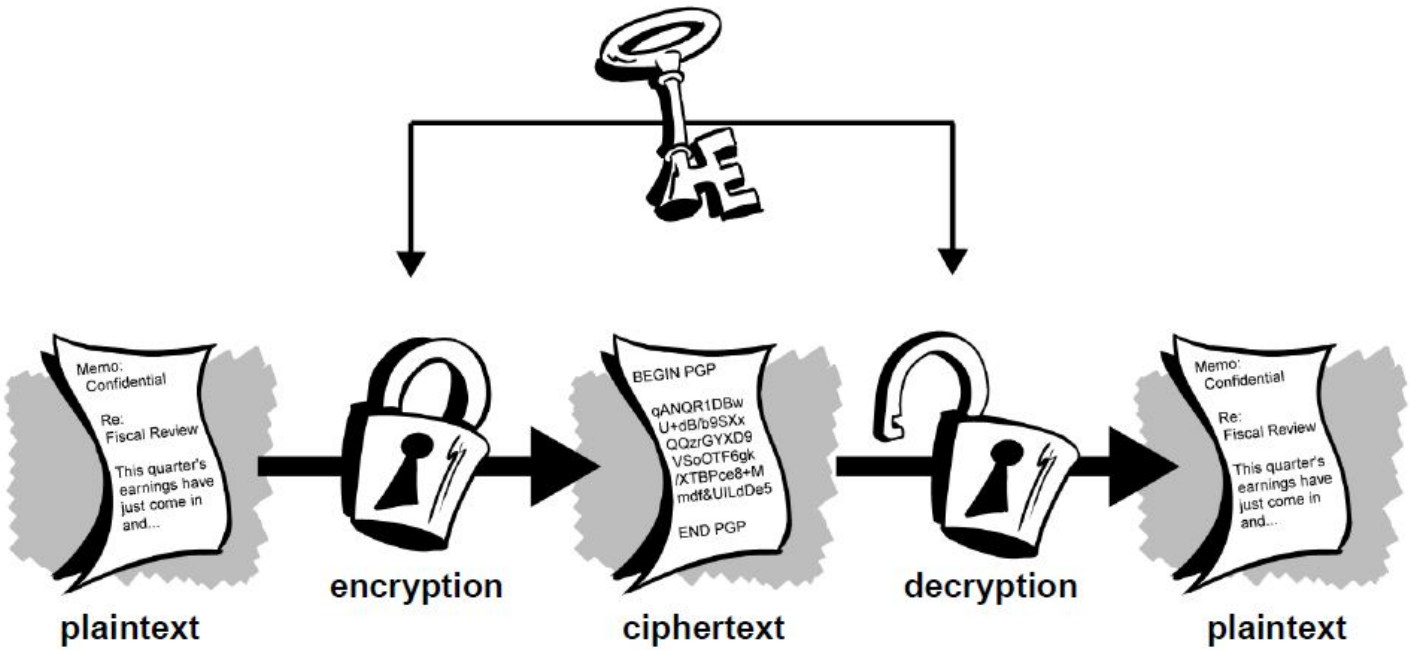
Valentin Ochs
a@0au.de

2017-02-27

Notwendigkeit der E-Mail-Verschlüsselung

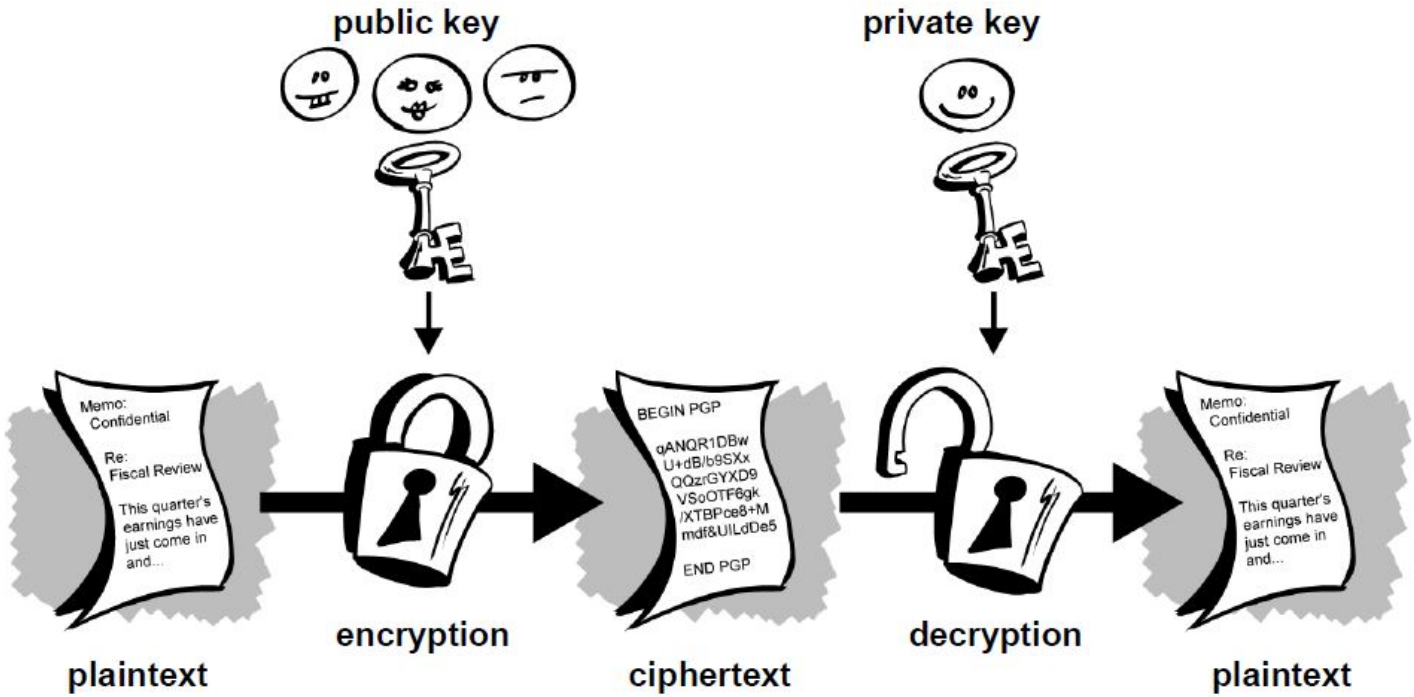
- Privatsphäre
- §110 Telekommunikationsgesetz: automatisiertes Überwachen der Telekommunikation durch berechtigte Stellen
- Abfangen von E-Mail-Nachrichten im lokalen Netz
- viele E-Mail-Nachrichten konzentriert auf Festplatte gespeichert
- aktuelle Entscheidung StB 34/07 des BGH: Verschlüsselung von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

Symmetrische Verschlüsselung



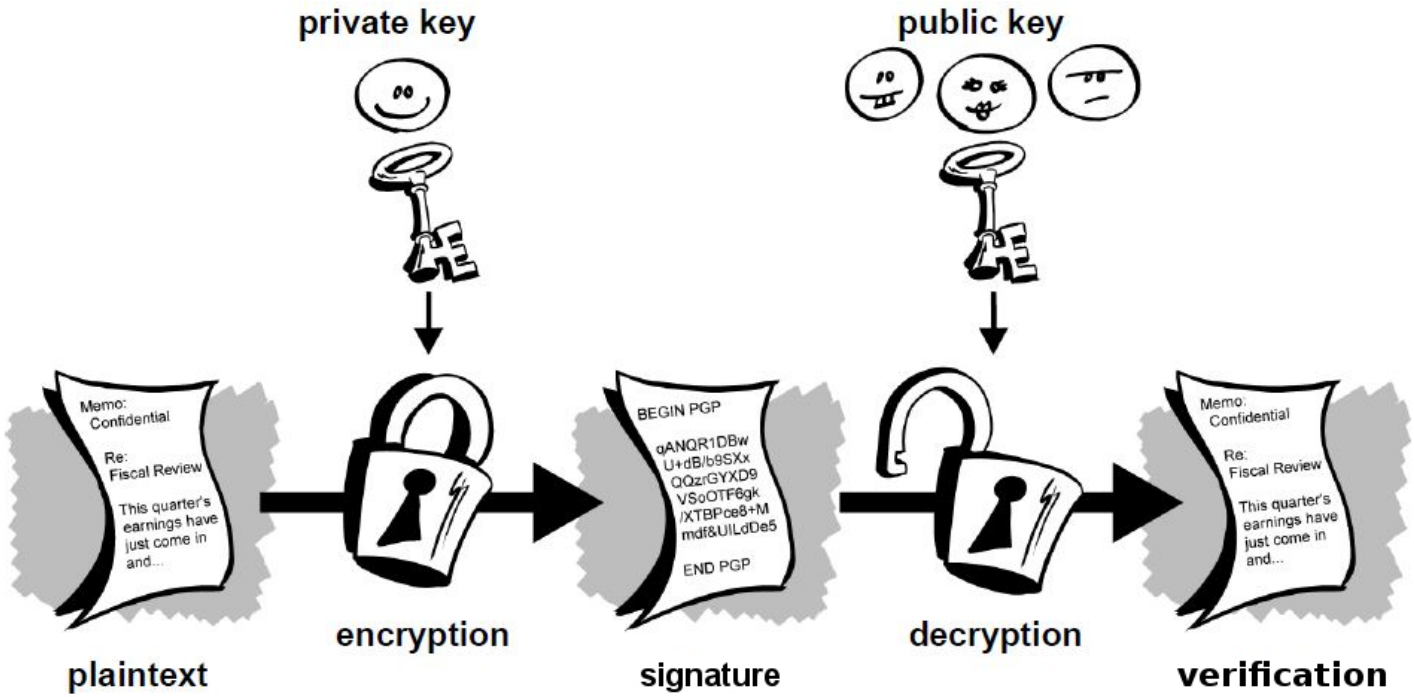
Analogon: Tresor mit Schlüssel

Asymmetrische Verschlüsselung



Analogon Verschlüsselung: Briefkasten mit Schlüssel
Anwendung eines Schlüssels hebt jeweils den anderen auf!

Signierung



Analogon Signatur: Vitrine mit Schlüssel

Praxis der asymmetrischen Verschlüsselung

Valentin Ochs
a@0au.de

- Jeder Teilnehmer hat ein Schlüsselpaar
- Schlüsselpaar: öffentlicher und privater Schlüssel, Briefkasten und Schlüssel
- Öffentliche Schlüssel werden untereinander getauscht und authentifiziert
- Private Schlüssel werden geheim gehalten

OpenPGP

- 1991 wird PGP 1.0 (Pretty Good Privacy) von Phil Zimmermann als Freeware veröffentlicht
- 1993 beginnen Ermittlungen gegen Zimmermann wegen angeblichen Verstoßes gegen US-Exportkontrollgesetze
- 1996 werden Ermittlungen eingestellt
- 1996 beschreibt RFC 1991 das Nachrichtenformat von PGP 2.6 mit RSA, IDEA, MD5
- 1998 beschreibt RFC 2440 das OpenPGP-Nachrichtenformat ab PGP 5.0
- 1999 erscheint GnuPG 1.0
- 2000 läuft das RSA-Patent aus, GnuPG 1.0.3 bekommt eine RSA-Implementierung
- 2007 löst RFC 4880 RFC 2440 ab

GnuPG

GNU Privacy Guard ist ein OpenPGP-kompatibles Programm...

- zur Erzeugung und Verwaltung von Schlüsselpaaren
- zum Ver- und Entschlüsseln von Dateien
- zum Signieren und Verifizieren von Dateien
- zum Beglaubigen (= Signieren) fremder Schlüssel

Er bietet selbst keine graphische Oberfläche, dafür verwenden wir heute Enigmail.

OpenPGP Schlüssel

- Algorithmen und Schlüssellänge nach Bedarf wählbar
- Private Schlüssel durch Passwort (oder -satz) geschützt
- Gültigkeit durch zeitliche Frist oder manuellen Widerruf begrenzt
- Austausch durch Keyserver, die untereinander synchronisiert sind

Ursprung des öffentlichen Schlüssels

- Bob lädt seinen öffentlichen Schlüssel im Internet hoch
- Alice möchte Bob verschlüsselte Nachrichten schicken und lädt den Schlüssel runter

Ursprung des öffentlichen Schlüssels

- Bob lädt seinen öffentlichen Schlüssel im Internet hoch
- Alice möchte Bob verschlüsselte Nachrichten schicken und lädt den Schlüssel runter
- Mallory tauscht vorher den Schlüssel gegen seinen eigenen und fängt Alices Nachrichten ab

Ursprung des öffentlichen Schlüssels

- Bob lädt seinen öffentlichen Schlüssel im Internet hoch
- Alice möchte Bob verschlüsselte Nachrichten schicken und lädt den Schlüssel runter
- Mallory tauscht vorher den Schlüssel gegen seinen eigenen und fängt Alices Nachrichten ab
- . . . und kann sie jetzt in Ruhe lesen und verändern, da die Nachrichten mit Mallorys Schlüssel verschlüsselt sind.

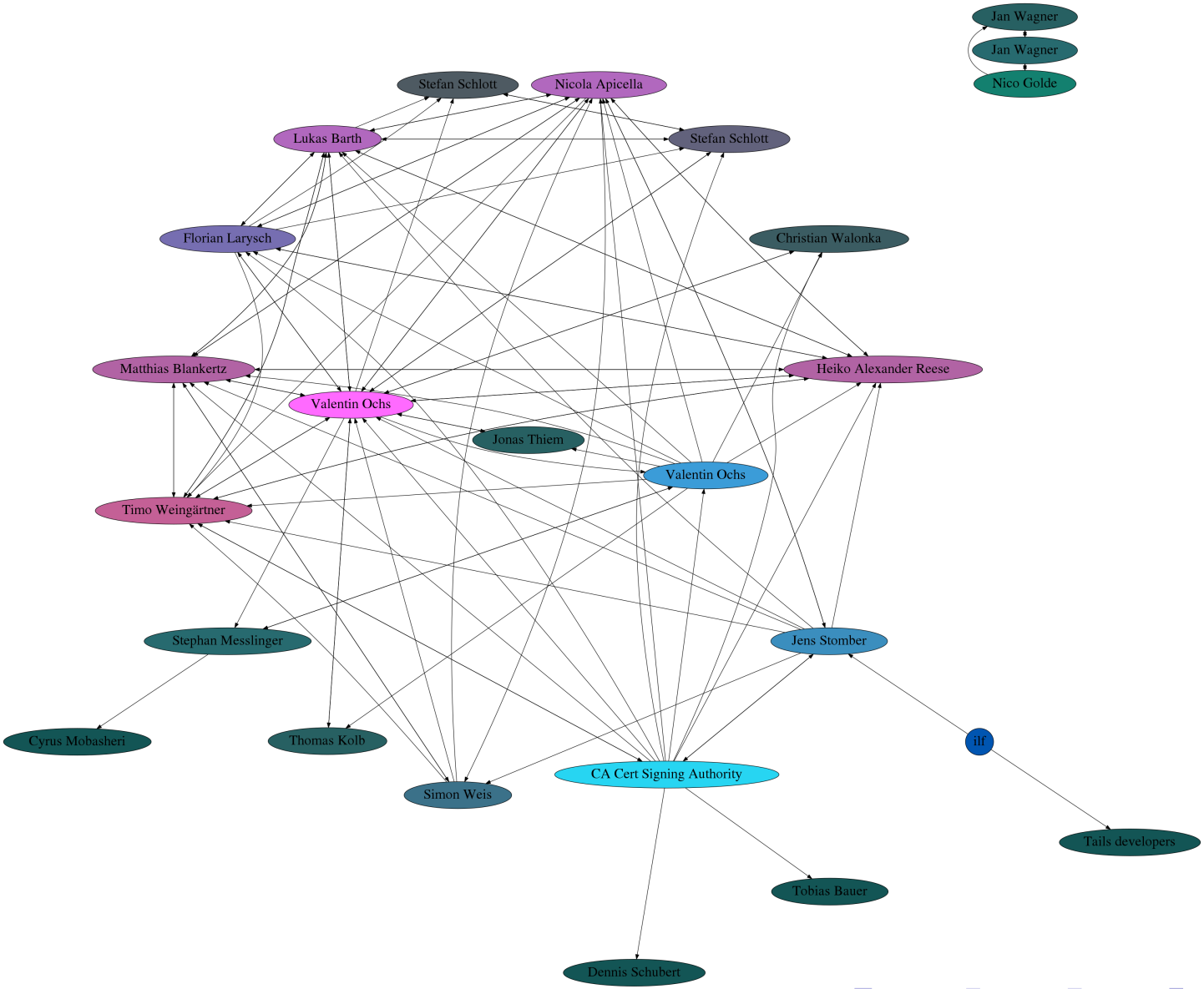
Fingerabdruck

- Bob sagt vorher Alice in Person "Mein Schlüssel hat den Fingerabdruck 12345678"
  - Fingerabdruck: z.B. die letzten Ziffern des Schlüssels
  - In Realität komplizierter, prüft den ganzen Schlüssel, nicht nur die letzten Ziffern
  - Austausch mündlich, per Visitenkarte, bei Crypto/Key Signing Parties...
  - Hauptsache man weiß wirklich, mit wem man redet, und dass es nicht abgefangen werden kann
- Vertrauen nur bei richtigem Fingerabdruck
- Modifikationen werden bemerkt

Web of Trust

- Alice vertraut Bob absolut
- Bob lädt eine von ihm signierte Nachricht ins Internet “Der Schlüssel von Charlie endet mit den Ziffern DEADBEEF”
- Alice kann jetzt auch Charlies Schlüssel vertrauen

Web of Trust


Jan Wagner
Jan Wagner
Nico Golde
Stefan Schlott
Nicola Apicella
Lukas Barth
Stefan Schlott
Florian Larysch
Christian Walonka
Matthias Blankertz
Heiko Alexander Reese
Valentin Ochs
Jonas Thiem
Valentin Ochs
Timo Weingärtner
Stephan Messlinger
Jens Stomber
Cyrus Mobasheri
Thomas Kolb
ilf
CA Cert Signing Authority
Simon Weis
Tails developers
Tobias Bauer
Dennis Schubert

Beispiel PGP Nachricht

-----BEGIN PGP MESSAGE-----

owGbwMvMwMEY0XWlWpZt30zGNeJJLGmZOakRO8UOeqTm5OTrKJTnF+
MHIwyIopsmxtmCb4QUN15wdmCVWYTlYmkBYGLk4BmMi22+z/410zRD
R21LKo/mp/wiI46nS0p6bYRlslhL4tjnW72eFp5SmDdFfZrP6dB8Vw
b756P1tsfYXDObvMD28dD63KDVrHaHWDefnl8wtDtsakeEYqmmQImt
YcKckxZ97ot1N92tX31v4vdG04eRmUuVN80QUDwVcFXO7XrGq+busp
VnVGJdPdRewFq0SNXUhLXijrm91fVn2aM00w5qJ0S84+tskMhRpMtq
3WCZsfpBItsS+/PSxQtM9Hdv3Nl1Jkvz/dSctaorllySafusM+Ppti
2bpyW3D8TEaF5SetF9ekqLECAA==
=5Q3n
-----END PGP MESSAGE-----

Beispiel PGP Schlüssel

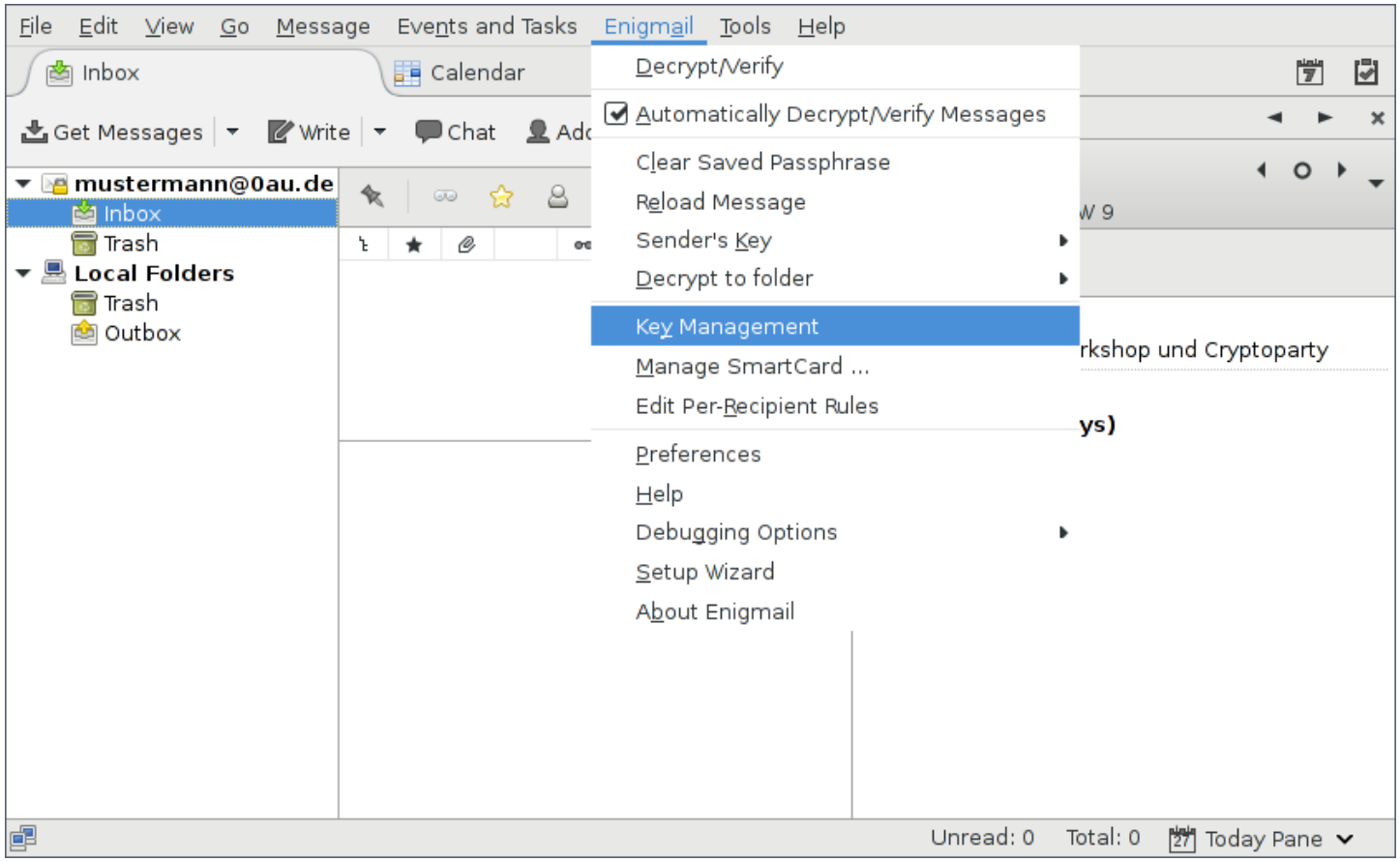
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFdJZrgBEAC4IMpmeE1/vbP4E+nI5Pgp2cSkFw6VbgW0T5ZNhF
WTCuP7Neq+Qt6xsYc2E1YK/1447PzjDvfLmHjiHS3APuX6PToYFO77
hJMjWCrXOnihOLEV/RpPGtI1hbhHjThLl2KsGpCWvAwDZX0cMS8yqB
q+84bLMC9T7A8QqwUkhsTv7h5wbILorHbYtbt594IYPbZF/PuqOTAA
v2zOl1pusiin3UgfbfdkS1C+Q6kZICkx/7j+9VqZhC4qbZ35nLpj1X
JPNmFhMnDt6SYwpr2IphMFV3KszHweXsJMoRkyJV335Wv/uYt5zmsd
6fixawbsvzsBJAi90JGUougVSSbedydKwYpf4u8PvFQqRGH6NqKy1X
nNE42Ak834FoLO9Jaj/xgW+3Y4dv9c4yzEvz+sjqZ/4E1I61PmPeyg
heF2FZr+WVsvakb+NRrHGkeEw4IGgauJNlEkDljaNt8G/0cio7wje3
uDbunPR9SDXvsETeClaLpJlfr9h/hYurQHXA5n8UNQFfBCrD4afjT8
9o+X9HMVEpxD65MxWx24vF46doL7+9c5cD70odlcP1Sg6LGtapensy
tBhWYWxlbnRpbiBPY2hzIDxhQDBhdS5kZT6JAj0EEwEKACcCGwEFCQ
F4AFAldKZ3AFCwkIBwMFFQoJCAsFFgMCAQACGkQiBbwGK3Kx4onuh
rT6kTF6fJLljF7HO6e5TQH7lgOjfvcNk1i2CFshVM6N+Q1EKACd9Oy

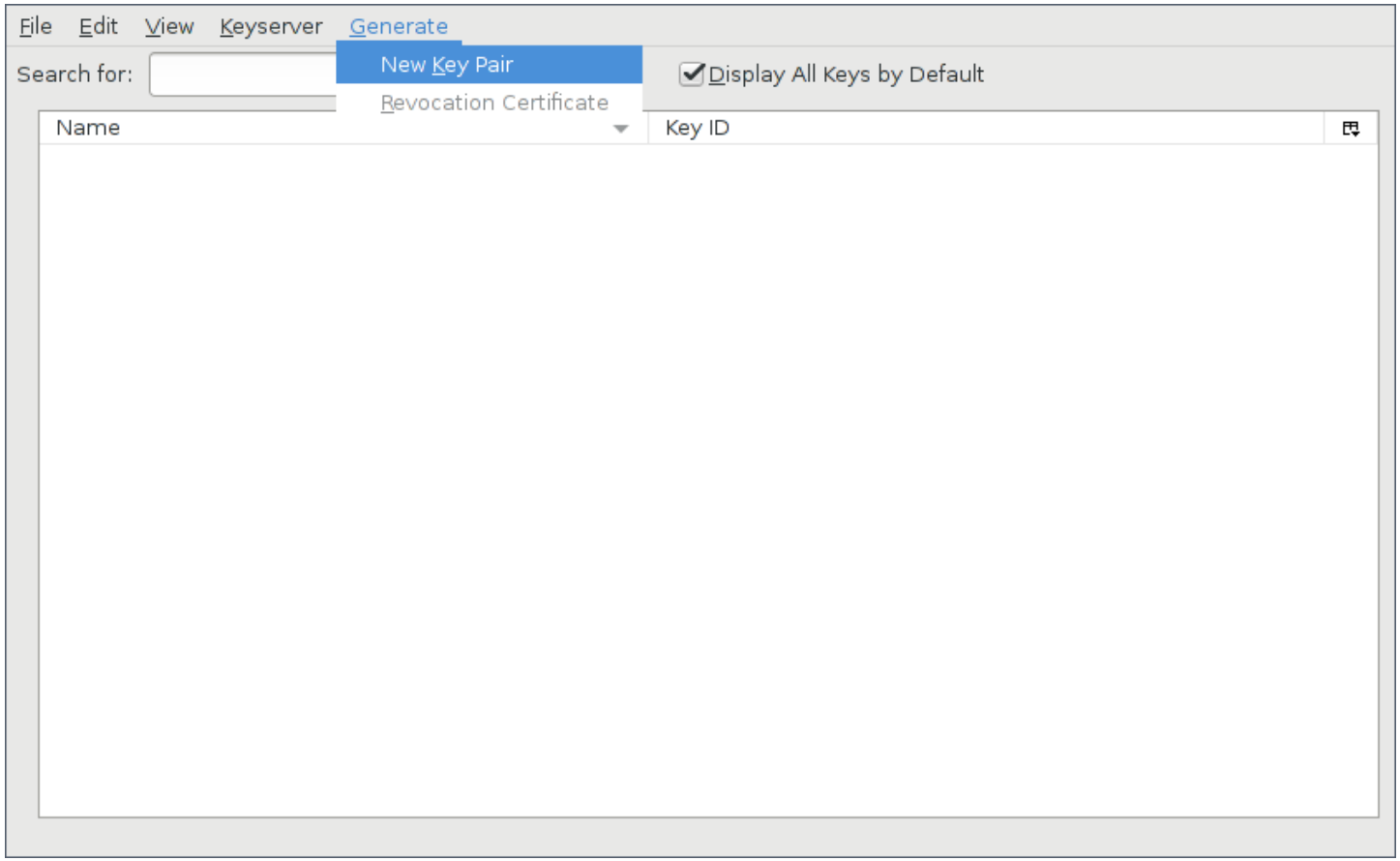
Was ist Enigmail

- Graphische Benutzeroberfläche für GnuPG
- Erweiterung für Thunderbird und SeaMonkey
- Open Source, also auf vielen Betriebssystemen verfügbar
- Alternativen:
  - WebPG für Firefox und Chrome
  - OpenKeychain + K9 für Android
  - GPG direkt verwenden :)

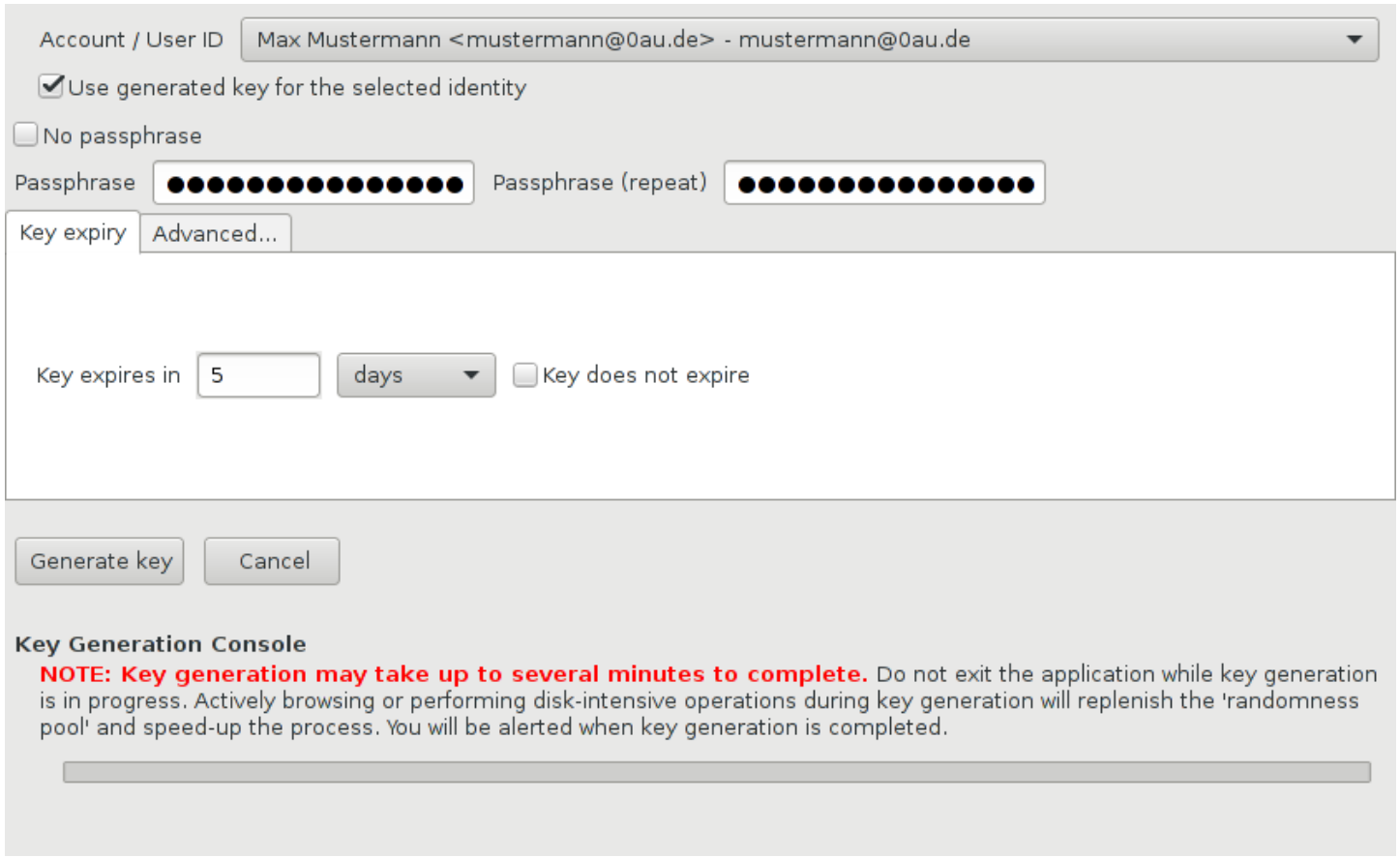
Menüeinträge



Starte Schlüsselerzeugung



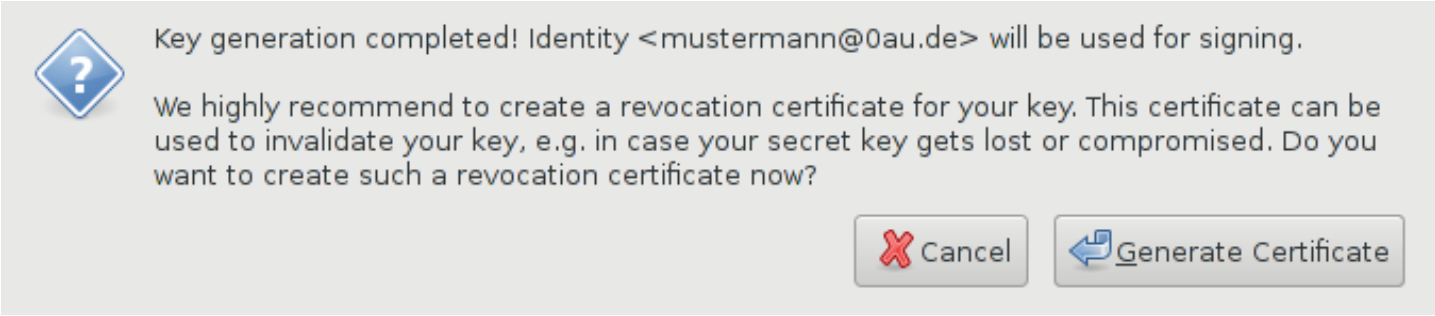
Erzeuge ein Schlüsselpaar (1/2)



Erzeuge ein Schlüsselpaar (2/2)

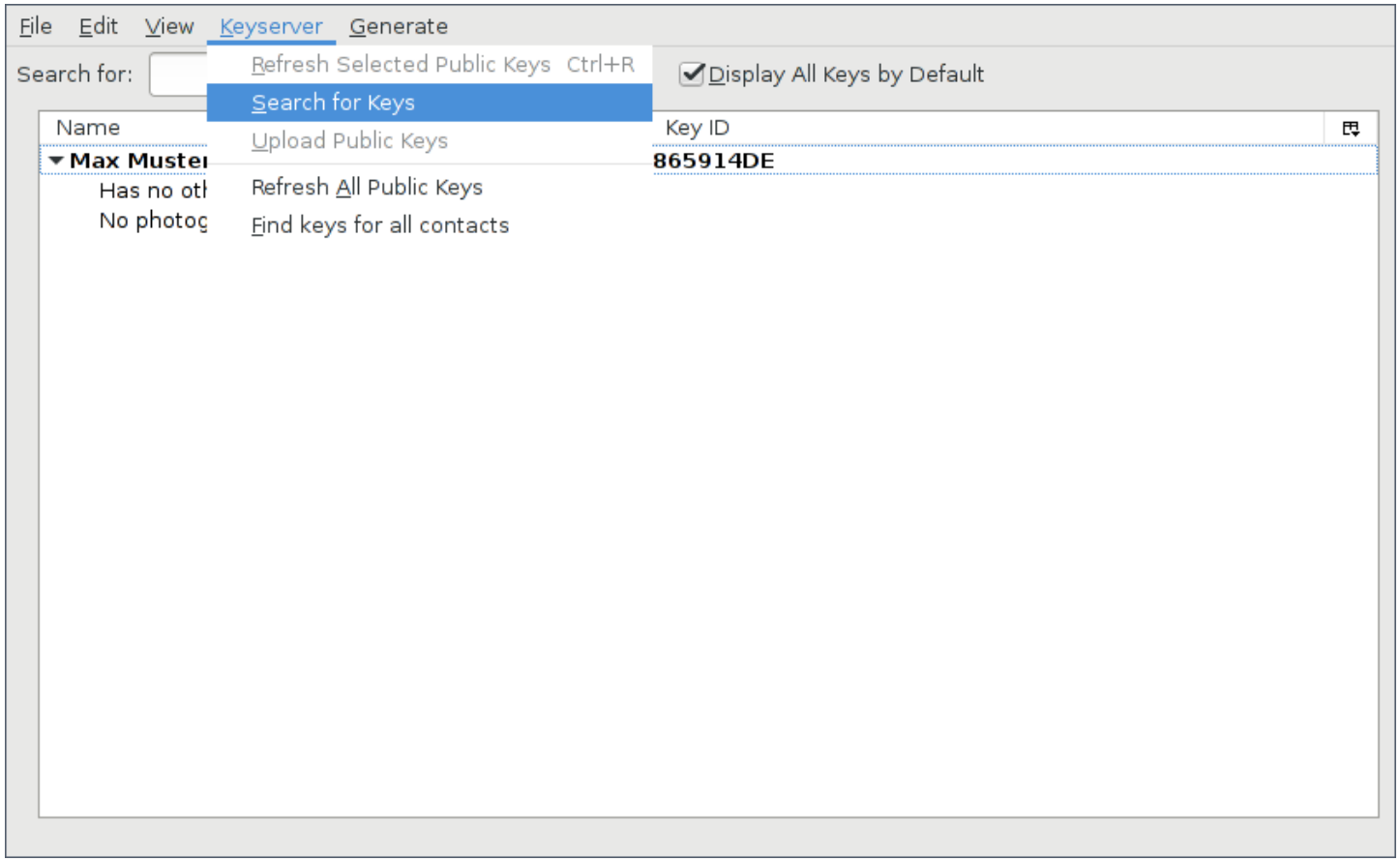
- Pseudonyme sind möglich, Enigmail verwendet allerdings die Kontoeinstellungen
- Ein Schlüssel kann mehrere Identitäten enthalten (und diese nach der Erzeugung ändern)
- Kombination von Identitäten nicht immer sinnvoll
- Gültigkeitsdauer nach Bedarf wählen

Erzeuge ein Widerrufszertifikat

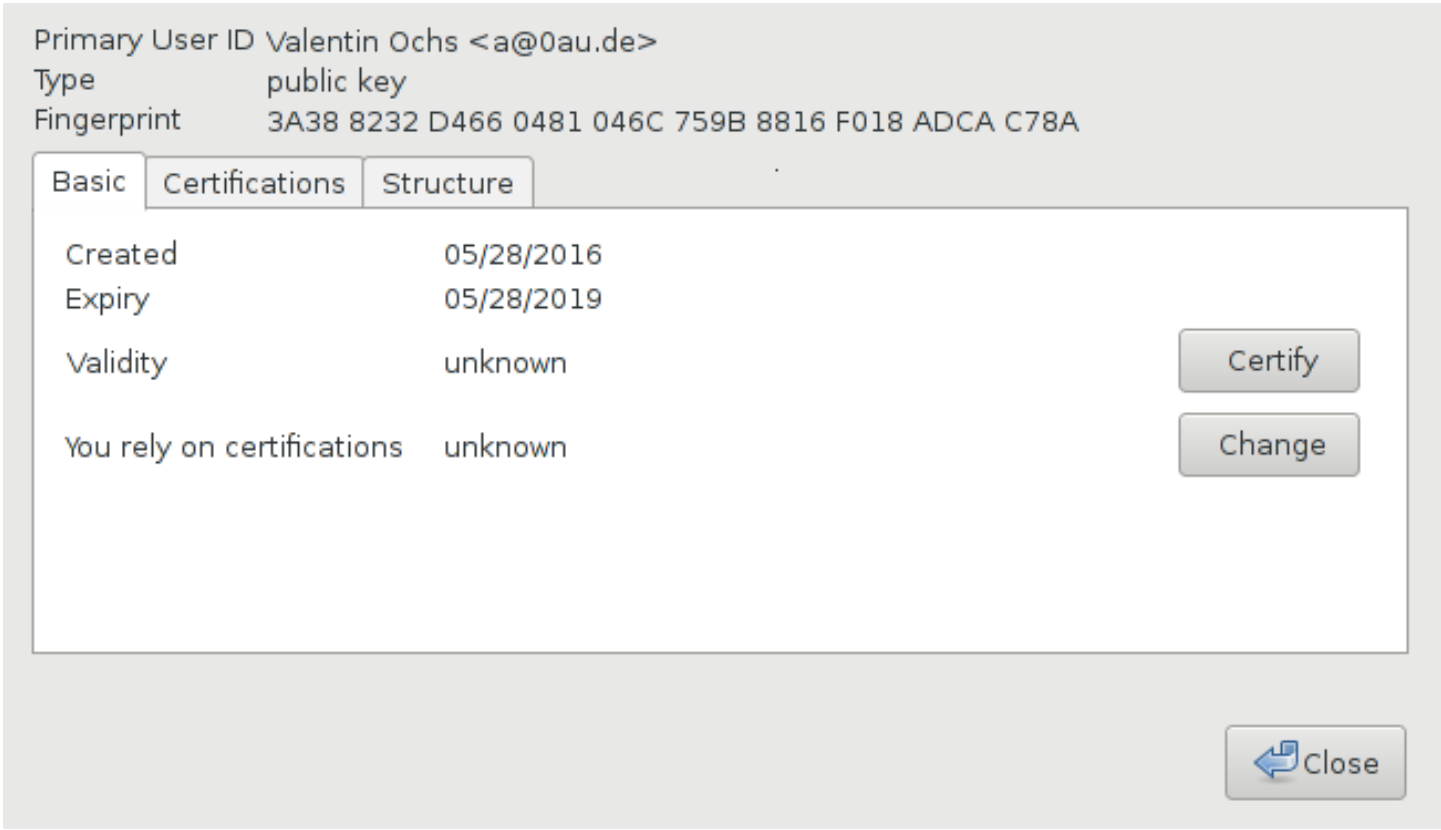


Das Widerrufszertifikat muss vor fremden Zugriffen sicher gespeichert werden. Durch Hochladen des Zertifikats wird der Schlüssel unwiderruflich als zurückgezogen markiert. Dies ist zB bei Verlust oder Kompromittierung des Schlüssels oder E-Mail-Adressen sinnvoll.

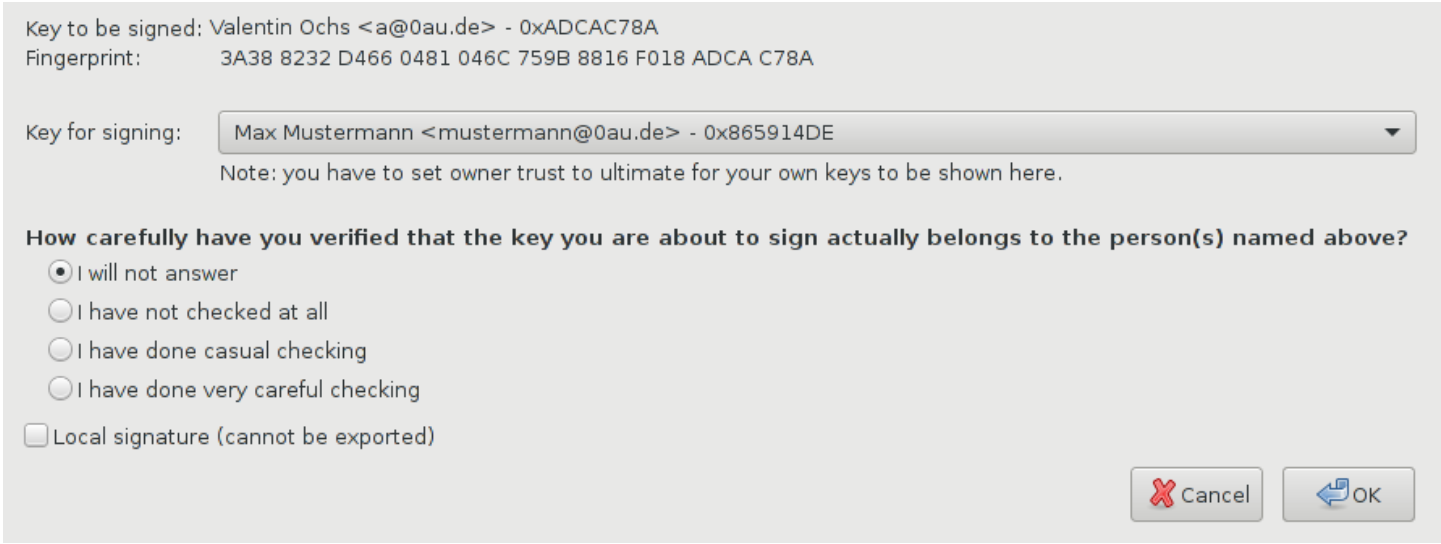
Import eines öffentlichen Schlüssels



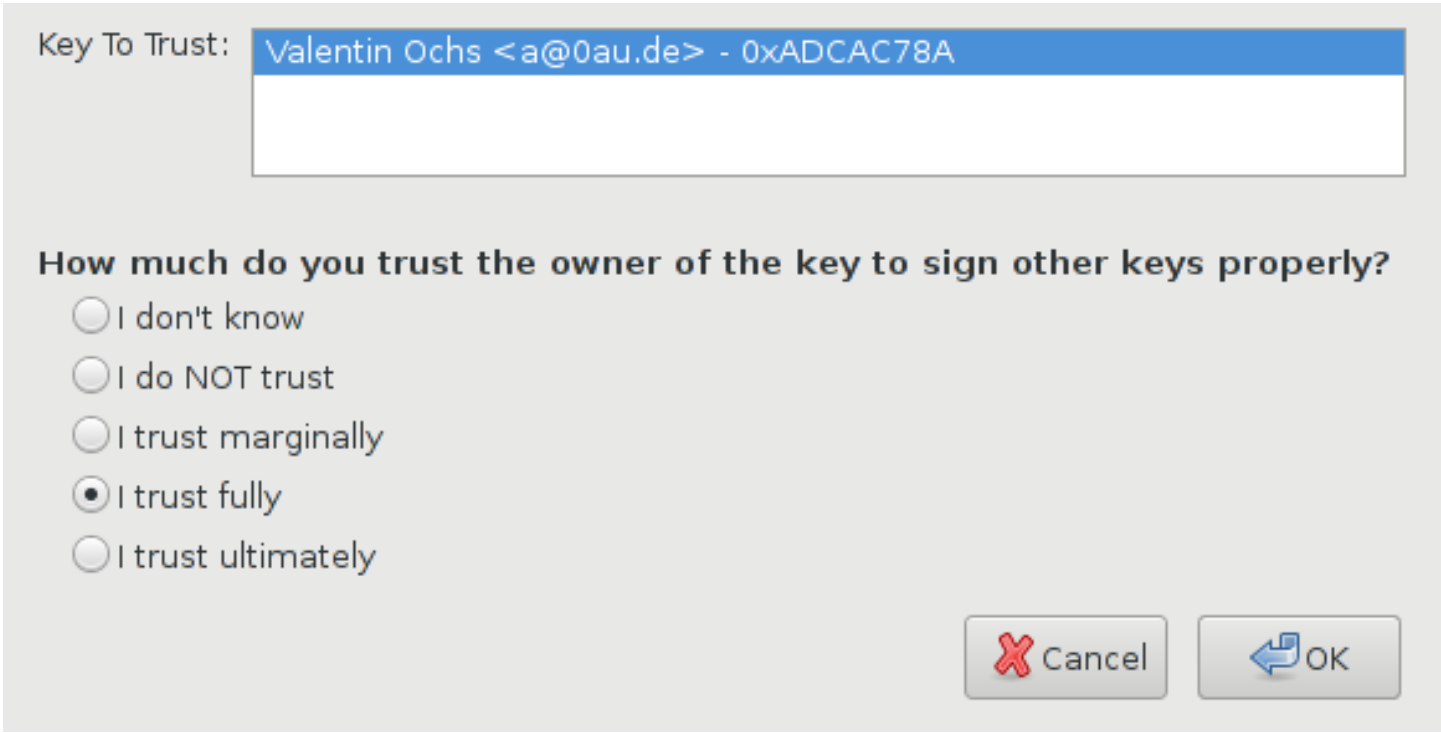
Schlüsseleigenschaften



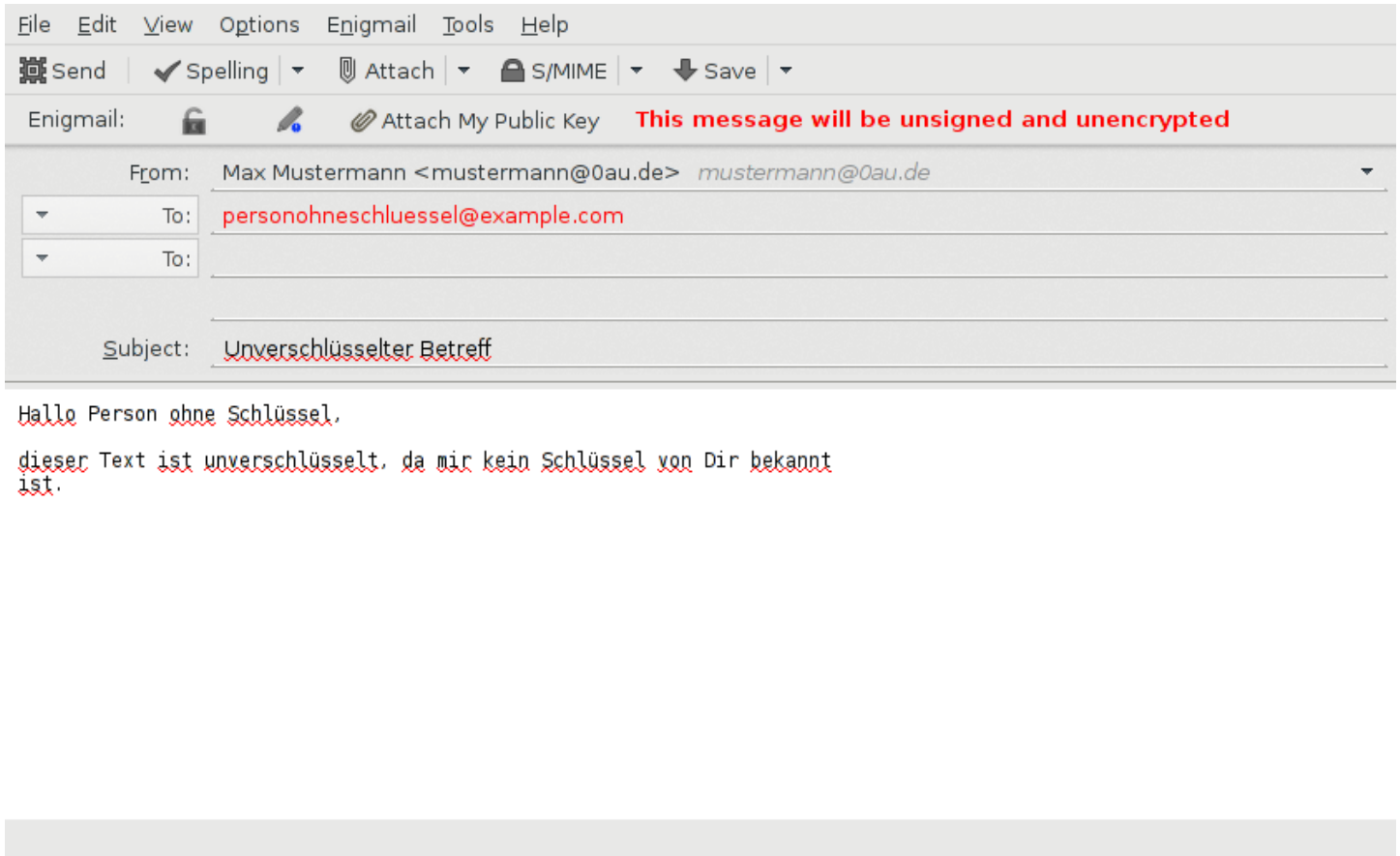
Beglaubigen eines Schlüssels (1/2)



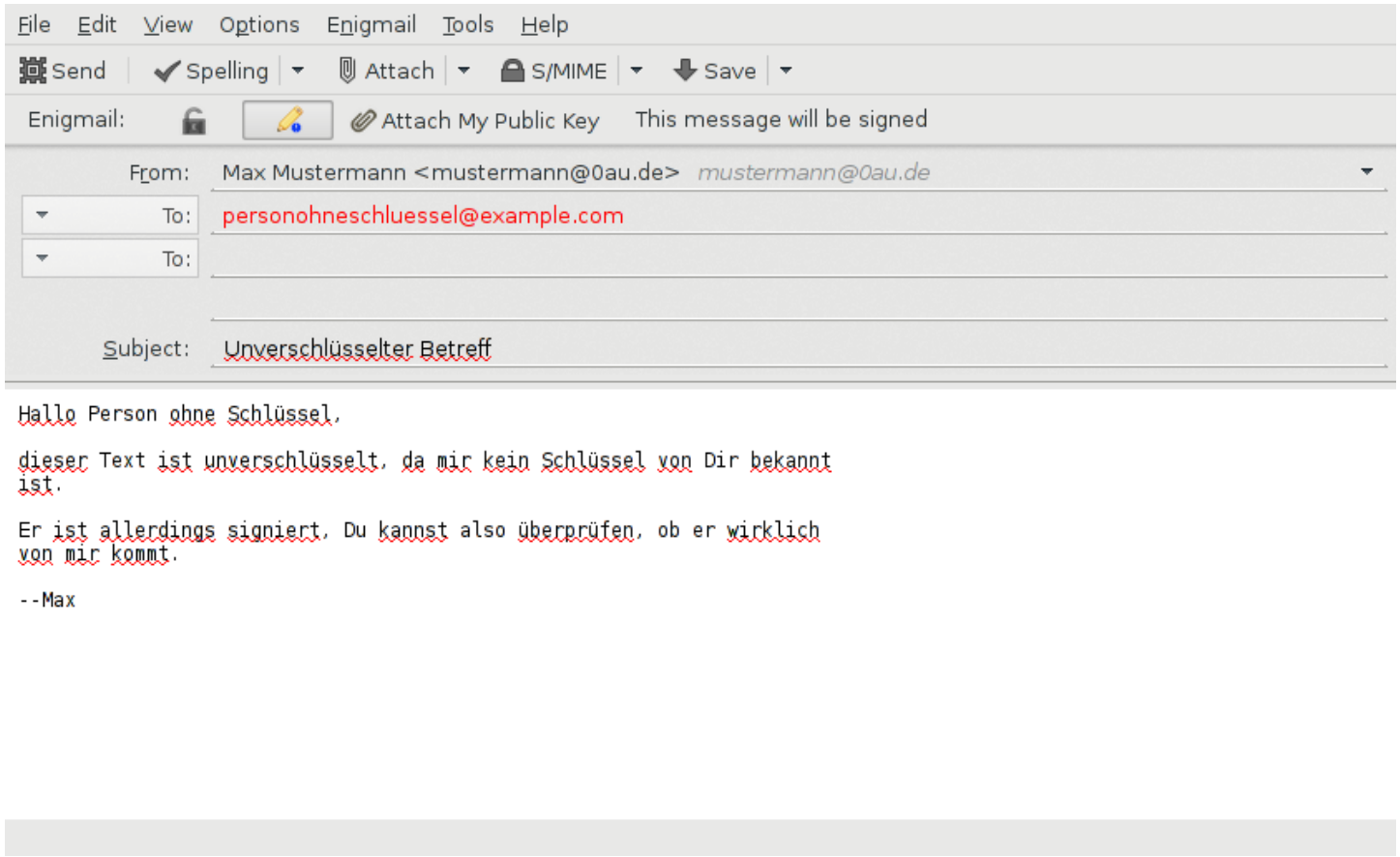
Beglaubigen eines Schlüssels (2/2)



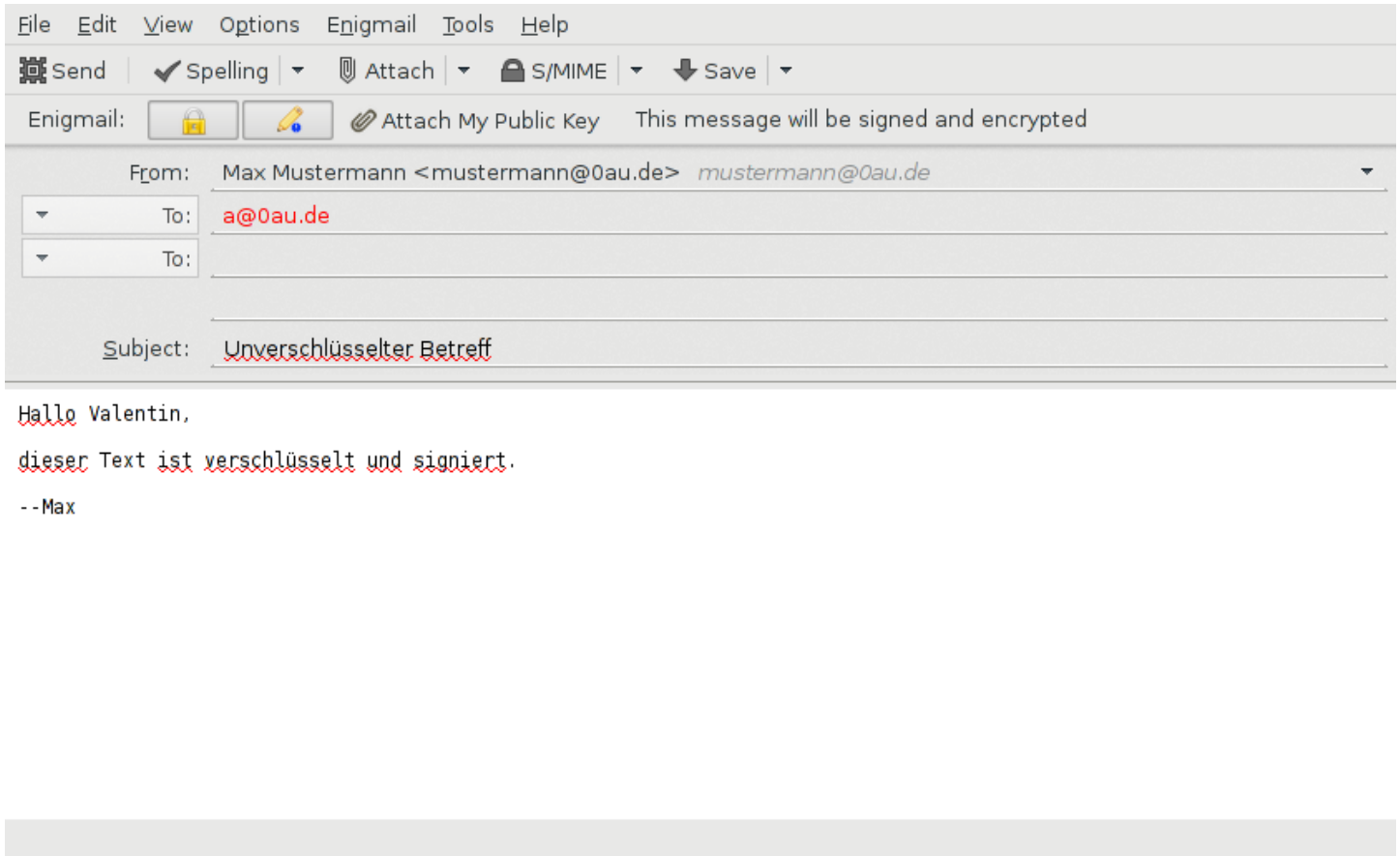
Schreiben von Mails (1/4)



Schreiben von Mails (2/4)



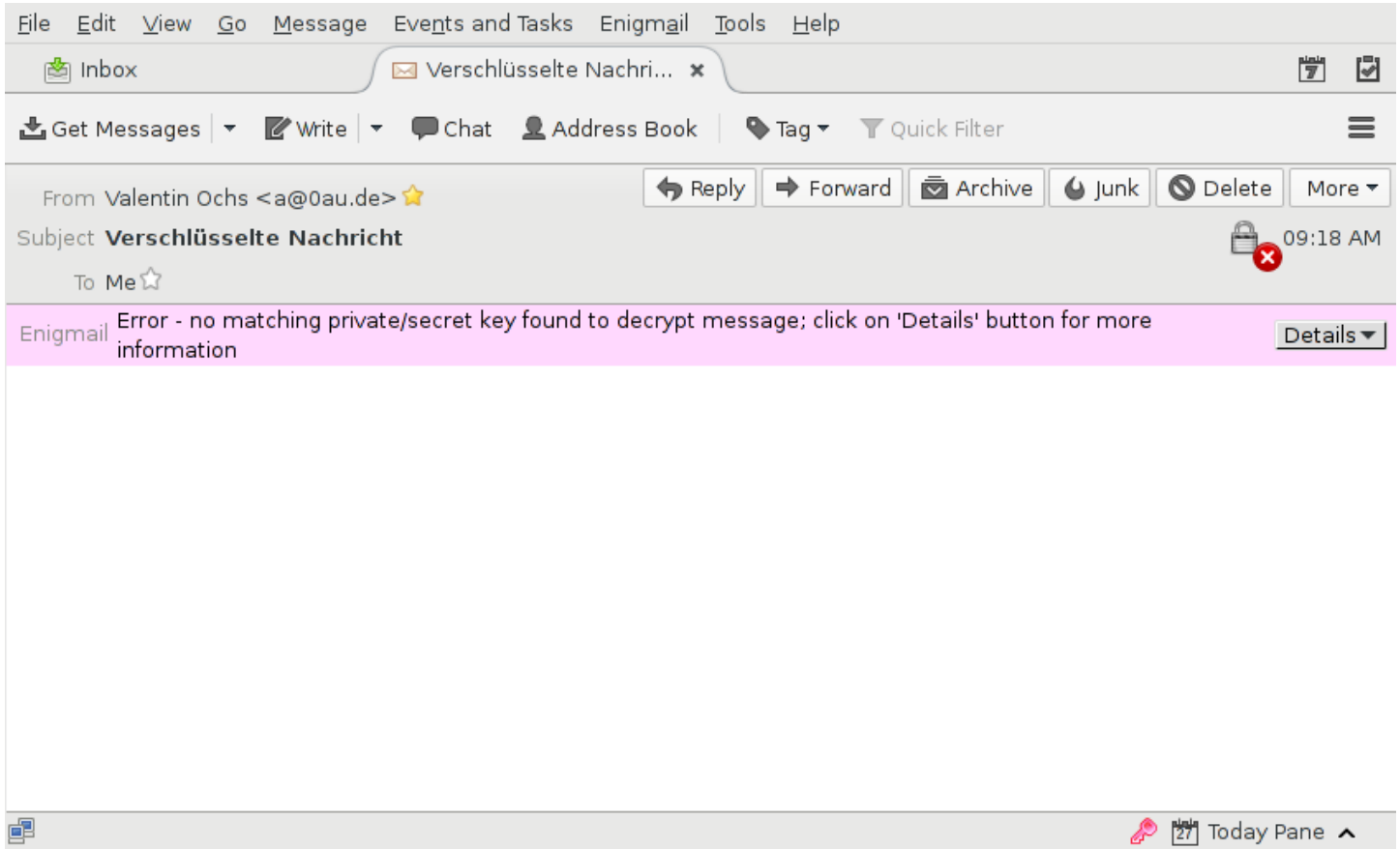
Schreiben von Mails (3/4)



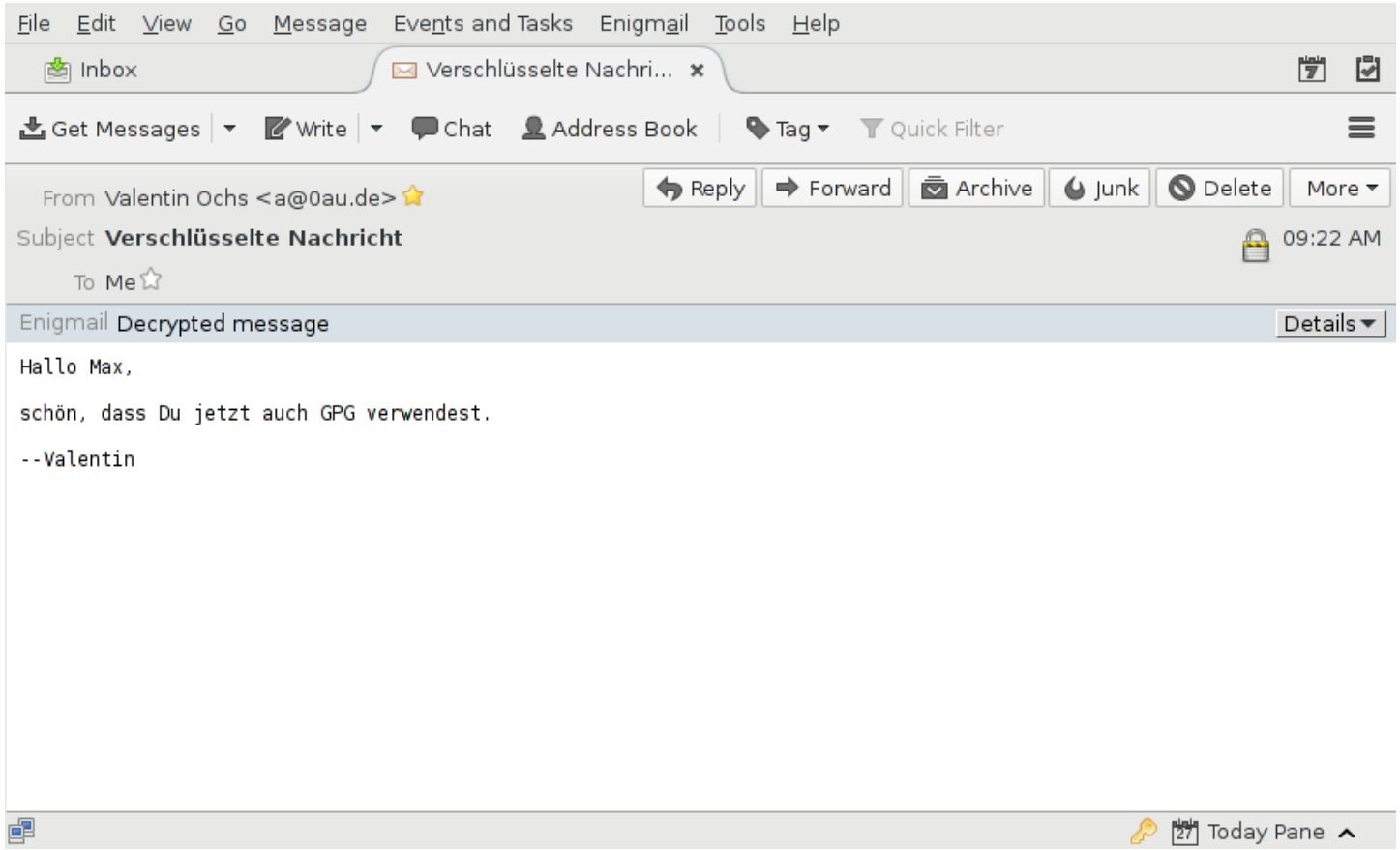
Schreiben von Mails (4/4)

Falls Anhänge verwendet werden, übernehmen diese automatisch die Einstellungen der Mail und werden mitverschlüsselt.

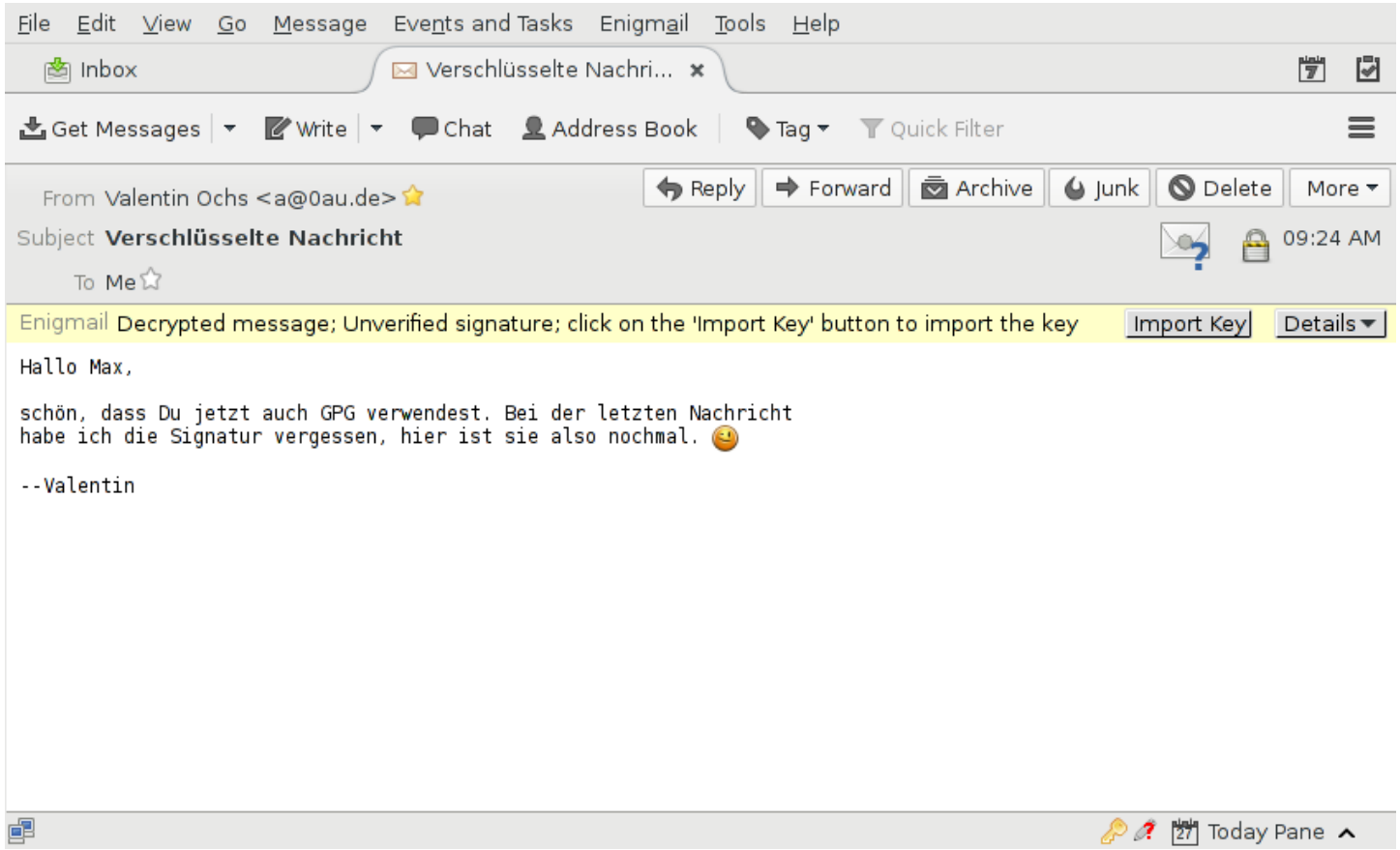
Anzeige einer unentschlüsselten Nachricht



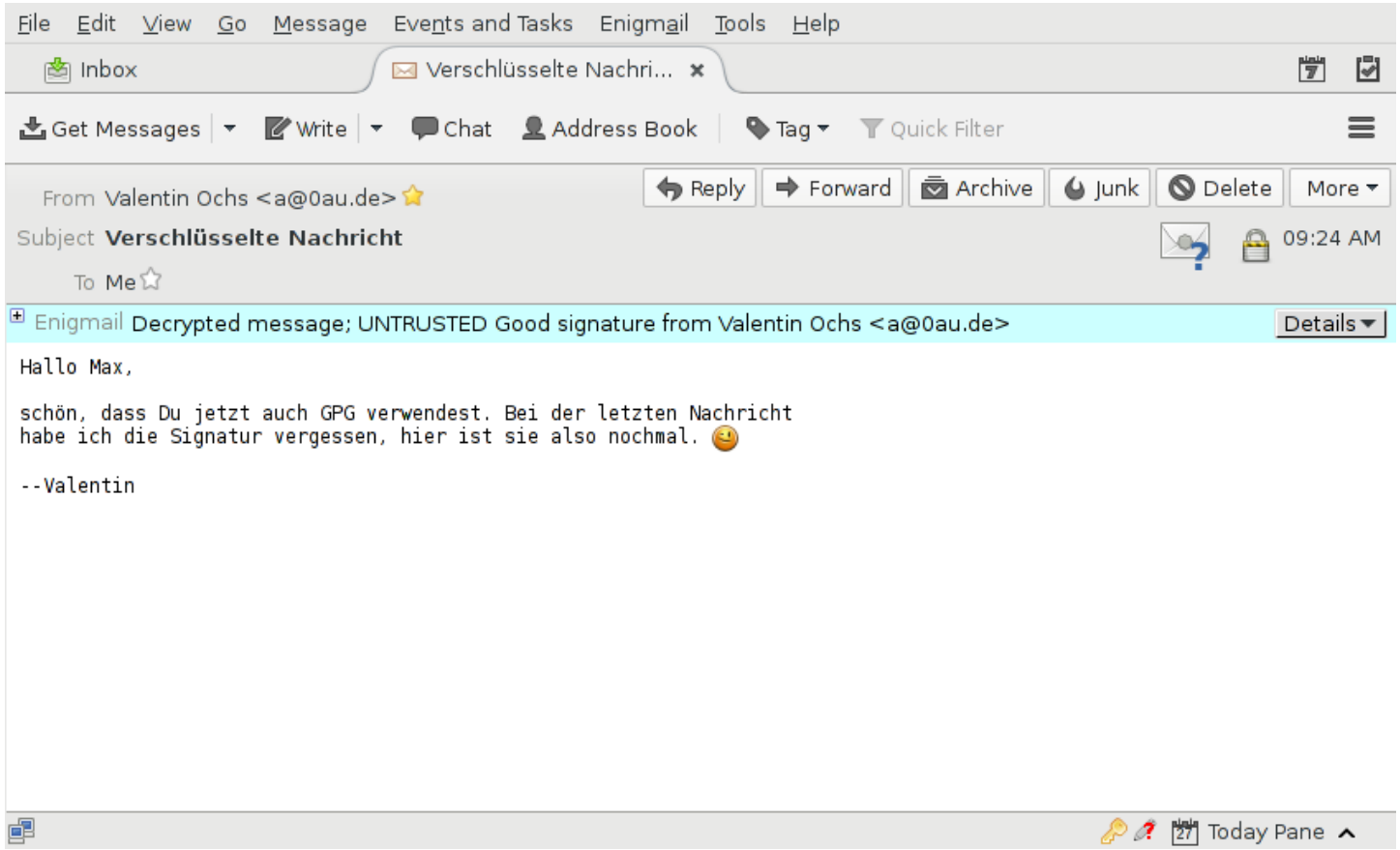
Anzeige einer entschlüsselten Nachricht ohne Signatur



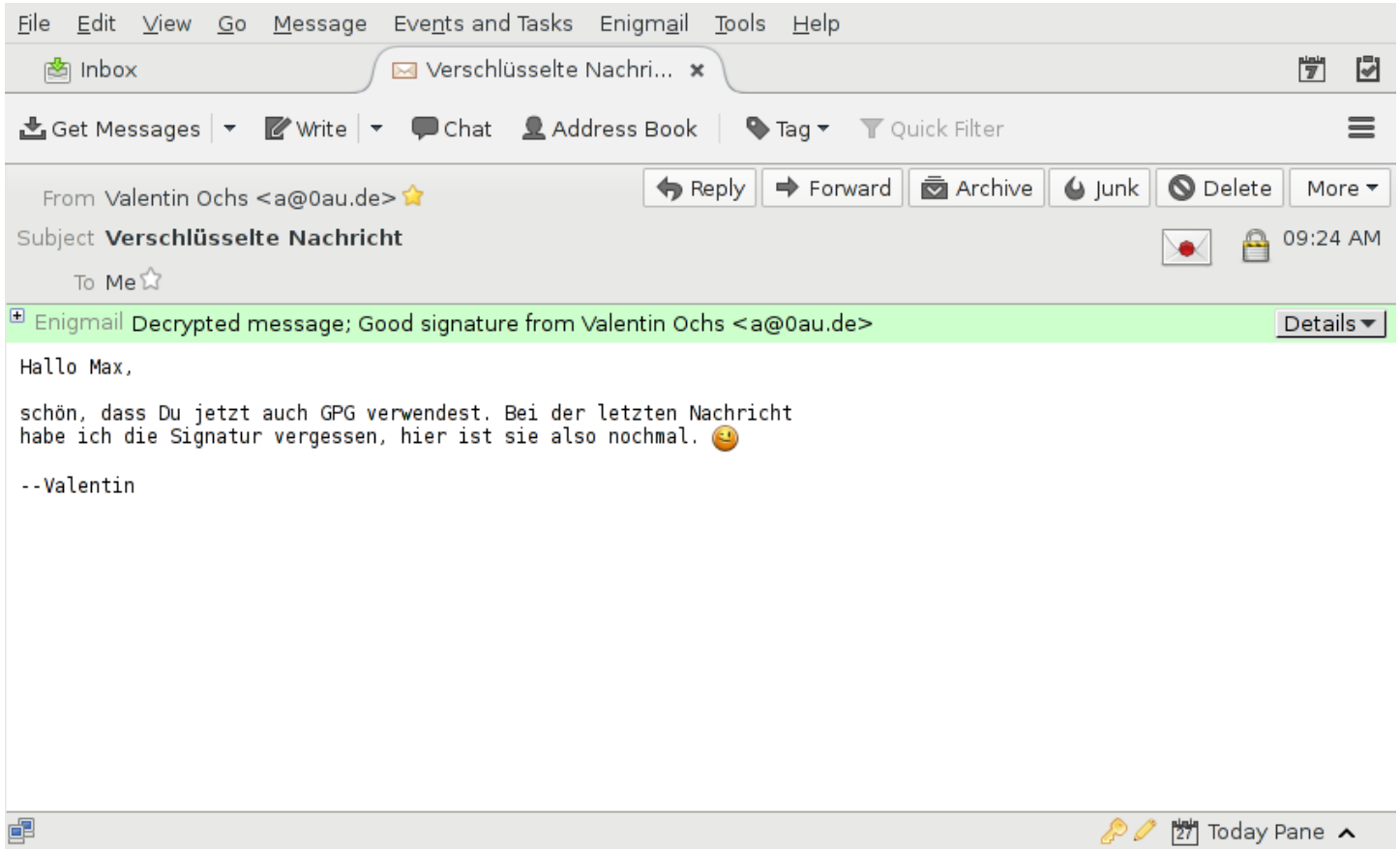
Anzeige einer entschlüsselten Nachricht (1/3)



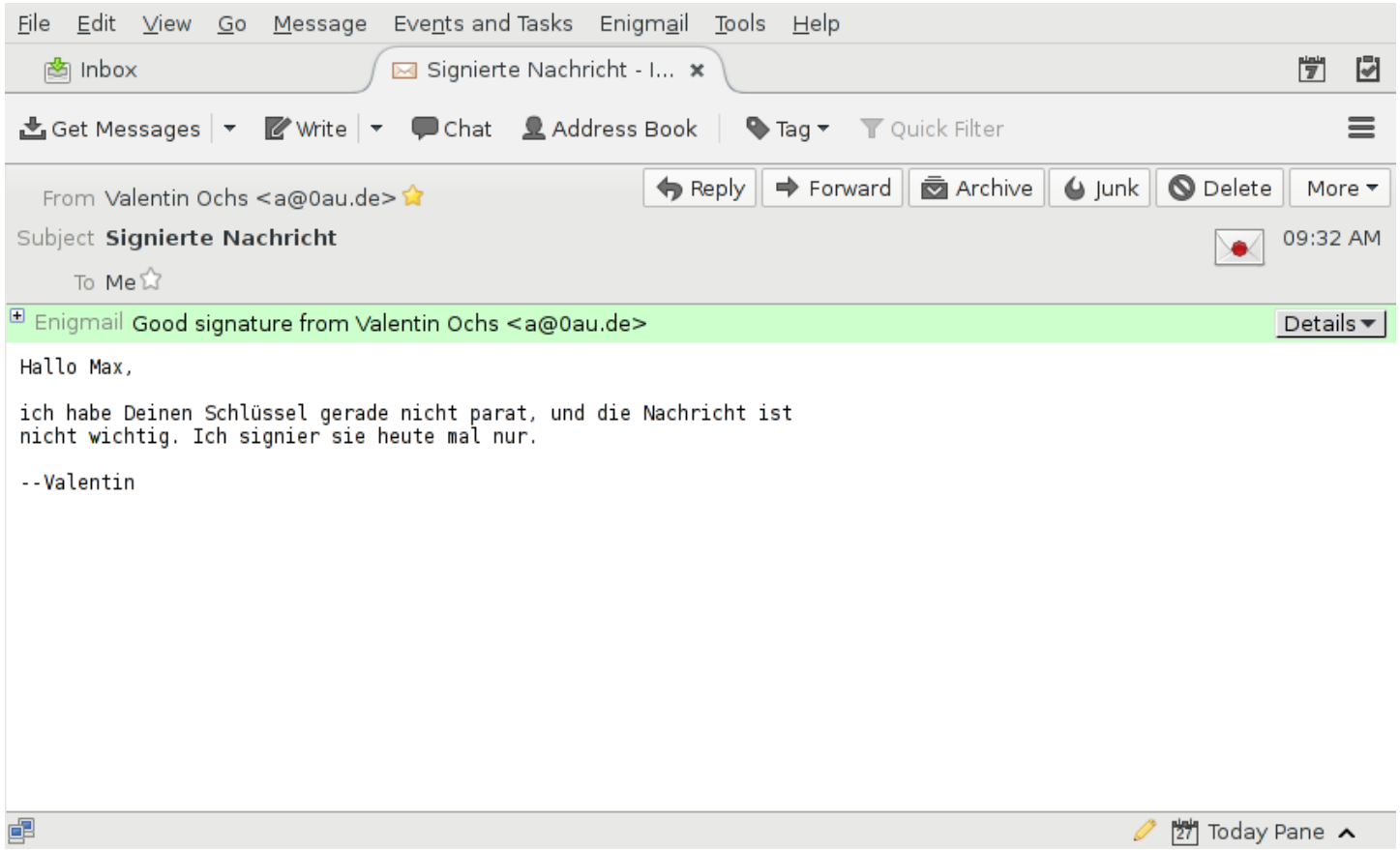
Anzeige einer entschlüsselten Nachricht (2/3)



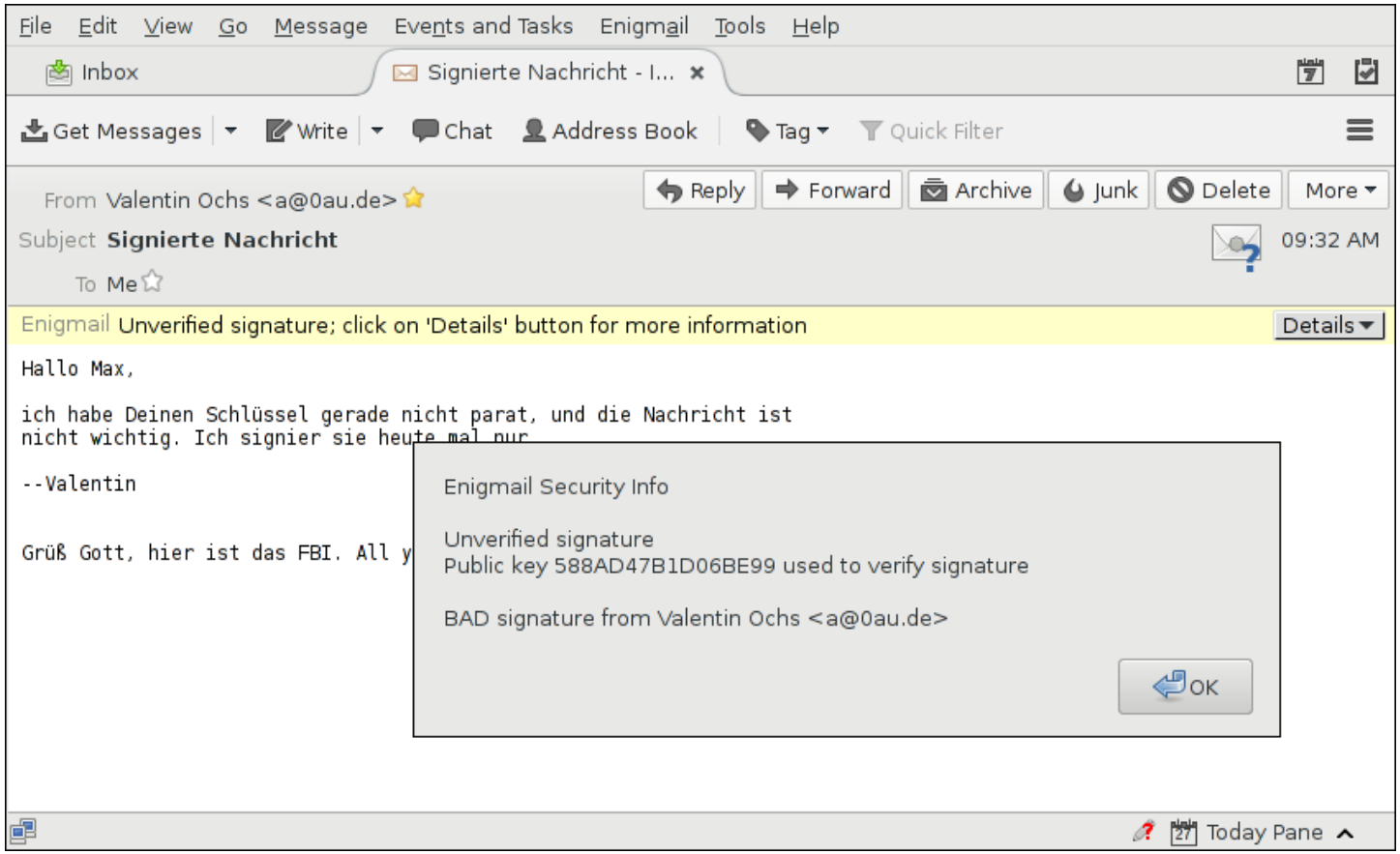
Anzeige einer entschlüsselten Nachricht (3/3)



Anzeige einer signierten Nachricht



Anzeige einer gefälschten Nachricht



Schlusswort

- Privaten Schlüssel und Widerrufszertifikat sicher speichern
- Privaten Schlüssel in einer sicheren Umgebung verwenden (Eigener Computer, Smartcard)
- Sicherheitslücken regelmäßig durch Updates schließen
- Verschlüsselung des Inhalts schützt nicht vor Auswertung von Metadaten
  - Verbindungsdaten
  - E-Mail-Header (z.B. Betreff)
  - Wer kommuniziert mit wem

Lizenz

Inhalte wurden teils aus einem 2008 gehaltenen Workshop von Christian Koch und Eric Goller übernommen.

Kontakt

Mail	a@0au.de
GPG	8816F018ADCAC78A
Fingerprint	3A388232D4660481046C759B8816F018ADCAC78A