

# E-Mail Verschlüsselung mit Enigmail

Valentin Ochs  
a@0au.de

2017-02-27

# Notwendigkeit der E-Mail-Verschlüsselung

E-Mail Verschlüsselung mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

Schlüsselverwaltung  
Nachrichten  
senden und  
empfangen

Ende

- 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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

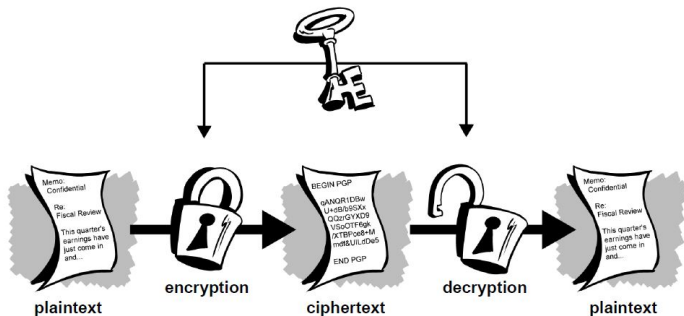
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



Analogon: Tresor mit Schlüssel

# Asymmetrische Verschlüsselung

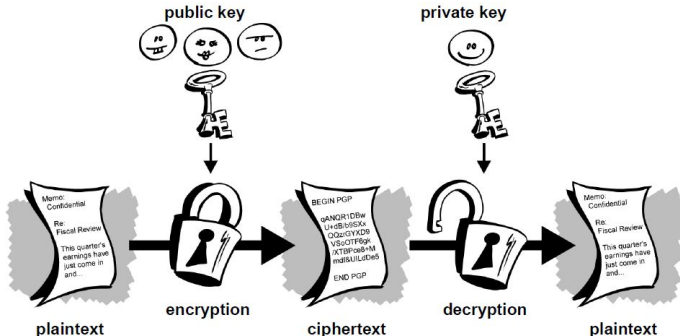
E-Mail Verschlüsselung mit Enigmail

Valentin Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselverwaltung  
Nachrichten senden und empfangen

Ende



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

# Signierung

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

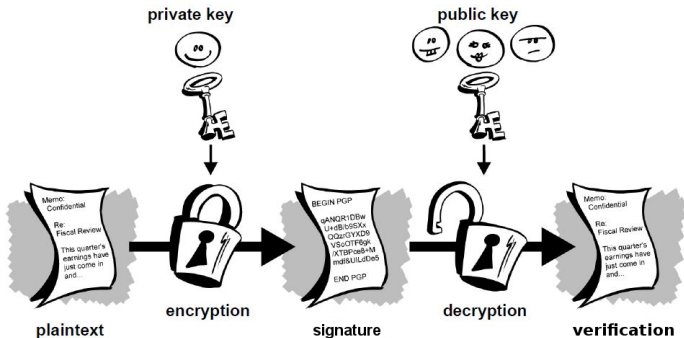
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



Analogon Signatur: Vitrine mit Schlüssel

# Praxis der asymmetrischen Verschlüsselung

E-Mail Verschlüsselung mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

Schlüsselverwaltung  
Nachrichten  
senden und  
empfangen

Ende

- 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

- 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

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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

- 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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

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

# Ursprung des öffentlichen Schlüssels

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

- 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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

- 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.

- 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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

- 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

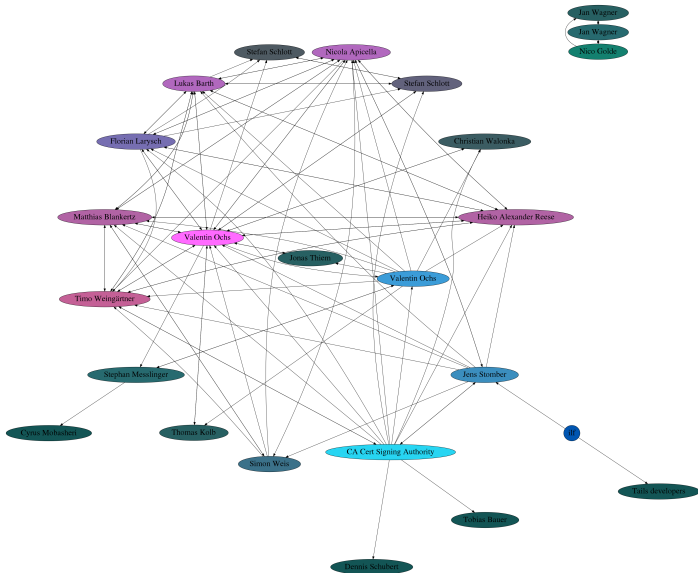
E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende



# Beispiel PGP Nachricht

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

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

owGbwMvMwMEY0XWlWpZt30zGNeJJLGmZOakR08U0eqTm50TrKJTnF+  
MHIwyIopsmxtmCb4QUN15wdmCVWYTlYmkBYGLk4BmMi22+z/410zRD  
R21LKO/mp/wiI46nS0p6bYRlslhL4tjnw72eFp5SmDdFfZrP6dB8Vw  
b756P1tsfYXD0bvMD28dD63KDvrHaHWDefnl8wtDtsakeEYqmmQImt  
YcKckxZ97ot1N92tX31v4vdG04eRmUuVN80QUdWvcFX07XrGq+busp  
VnVGJdPdRwFqOSNXUhLXijrm91fVn2aM00w5qJ0S84+tskMhRpMtq  
3WCZsfpBItsS+/PSxQtM9Hdv3Nl1Jkvz/dSctaorllySafusM+Ppti  
2bpyW3D8TEaF5SetF9ekqLECAA==  
=5Q3n

-----END PGP MESSAGE-----



# Beispiel PGP Schlüssel

E-Mail Verschlüsselung mit Enigmail

Valentin Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselverwaltung  
Nachrichten senden und empfangen

Ende

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

```
mQINBFdJZrgBEAC4IMpmeE1/vbP4E+nI5Pgp2cSkFw6VbgWOT5ZNhF
WTCuP7Neq+Qt6xsYc2E1YK/1447PzjDvfLmHjiHS3APuX6PToYF077
hJMjWCrXOnihOLEV/RpPGtI1hbhHjThL12KsGpCWvAwDZX0cMS8yqB
q+84bLMC9T7A8QqwUkhsTv7h5wbILorHbYtbt594IYPbZF/Puq0TAA
v2z0l1pusiin3UgfbfdkS1C+Q6kZICkx/7j+9VqZhC4qbZ35nLpj1X
JPNmFhMnDt6SYwpr2IphMFV3KszHweXsJMoRkyJV335Wv/uYt5zmsd
6fixawbsvzsBJAi90JGUougVSSbedydKwYpf4u8PvFQqRGH6NqKy1X
nNE42Ak834FoL09Jaj/xgW+3Y4dv9c4yzEvz+s jqZ/4E1I61PmPeyg
heF2FZr+WVsvakb+NRrHGkeEw4IGgauJN1EkDljaNt8G/0cio7wje3
uDbunPR9SDXvsETeClaLpJlfr9h/hYurQHXA5n8UNQFfBCrD4afjT8
9o+X9HMEpxD65MxWx24vF46doL7+9c5cD70odlcP1Sg6LGtapensy
tBhWYWxlbnRpbjBPY2hzIDxhQDBhdS5kZT6JAj0EEwEKACcCGwEFCQ
F4AFAl dKZ3AFCwkIBwMFFQoJCAsFFgMCAQAACgkQiBbwGK3Kx4onuh
rT6kTF6fJL1jF7H06e5TQH71g0jfvNk1i2CFshVM6N+Q1EKACd90y
```

# Was ist Enigmail

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

- 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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

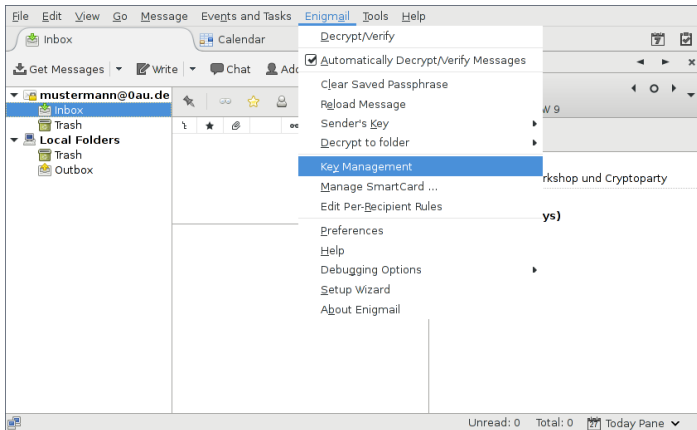
Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende



# Starte Schlüsselerzeugung

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

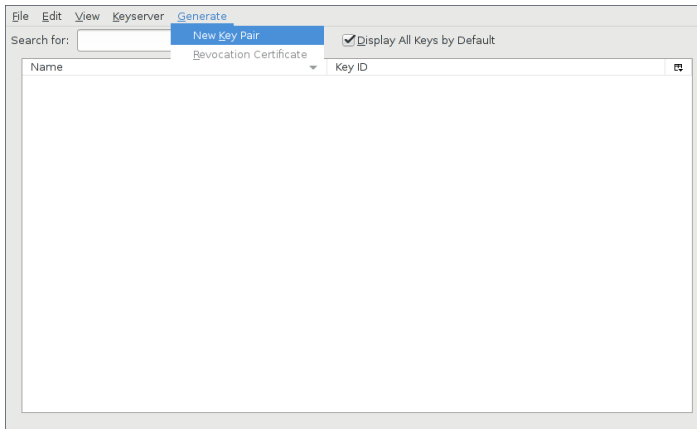
Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende



# Erzeuge ein Schlüsselpaar (1/2)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende

Account / User ID Max Mustermann <mustermann@0au.de> - mustermann@0au.de

Use generated key for the selected identity

No passphrase

Passphrase  Passphrase (repeat)

Key expiry

Key expires in    Key does not expire

**Key Generation Console**

**NOTE: Key generation may take up to several minutes to complete.** Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

# Erzeuge ein Schlüsselpaar (2/2)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende

- 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 Widerrufs-zertifikat

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen


Ende



Key generation completed! Identity <mustermann@0au.de> will be used for signing.

We highly recommend to create a revocation certificate for your key. This certificate can be used to invalidate your key, e.g. in case your secret key gets lost or compromised. Do you want to create such a revocation certificate now?

 Cancel

 Generate Certificate

Das Widerrufs-zertifikat 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

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

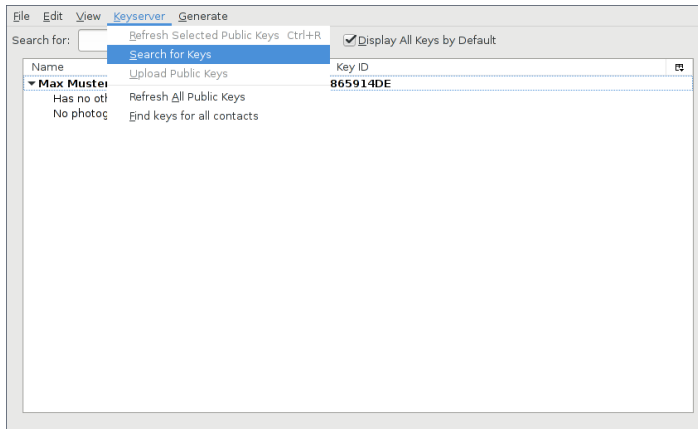
Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende





# Schlüsseleigenschaften

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende

Primary User ID Valentin Ochs <a@0au.de>

Type public key

Fingerprint 3A38 8232 D466 0481 046C 759B 8816 F018 ADCA C78A

Basic

Certifications

Structure

Created 05/28/2016

Expiry 05/28/2019

Validity unknown

You rely on certifications unknown

Certify

Change

Close

# Beglaubigen eines Schlüssels (1/2)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende

Key to be signed: Valentin Ochs <a@0au.de> - 0xADCAC78A  
Fingerprint: 3A38 8232 D466 0481 046C 759B 8816 F018 ADCA C78A

Key for signing: Max Mustermann <mustermann@0au.de> - 0x865914DE

Note: you have to set owner trust to ultimate for your own keys to be shown here.

**How carefully have you verified that the key you are about to sign actually belongs to the person(s) named above?**

- I will not answer
  - I have not checked at all
  - I have done casual checking
  - I have done very careful checking
- Local signature (cannot be exported)

 Cancel

 OK

# Beglaubigen eines Schlüssels (2/2)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

**Schlüsselver-  
waltung**

Nachrichten  
senden und  
empfangen

Ende

Key To Trust: Valentin Ochs <a@0au.de> - 0xADCAC78A

**How much do you trust the owner of the key to sign other keys properly?**



I don't know

I do NOT trust

I trust marginally

I trust fully

I trust ultimately

 Cancel  OK

# Schreiben von Mails (1/4)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

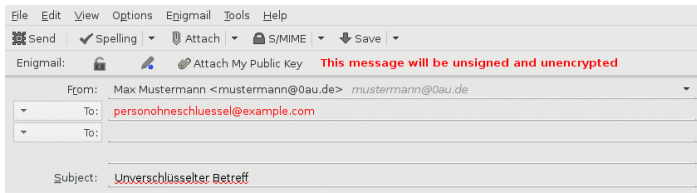
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



Hallo Person ohne Schlüssel.

dieser Text ist unverschlüsselt, da mir kein Schlüssel von Dir bekannt ist.

# Schreiben von Mails (2/4)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

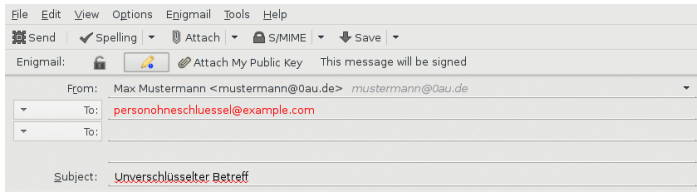
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



Hallo Person ohne Schlüssel.

dieser Text ist unverschlüsselt, da mir kein Schlüssel von Dir bekannt ist.

Er ist allerdings signiert. Du kannst also überprüfen, ob er wirklich von mir kommt.

--Max

# Schreiben von Mails (3/4)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

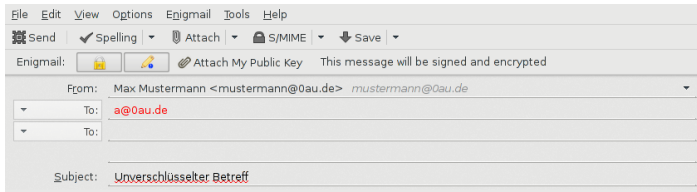
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



Hallo Valentin,  
dieser Text ist verschlüsselt und signiert.  
--Max

# Schreiben von Mails (4/4)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail

Schlüsselver-  
waltung

**Nachrichten  
senden und  
empfangen**

Ende

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

# Anzeige einer unentschlüsselten Nachricht

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

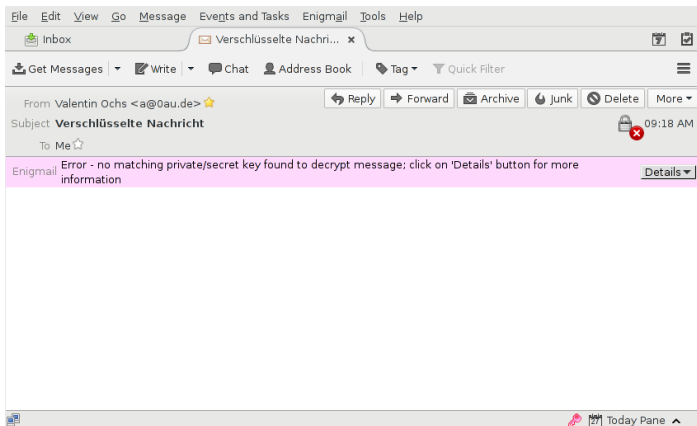
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende





# Anzeige einer entschlüsselten Nachricht ohne Signatur

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

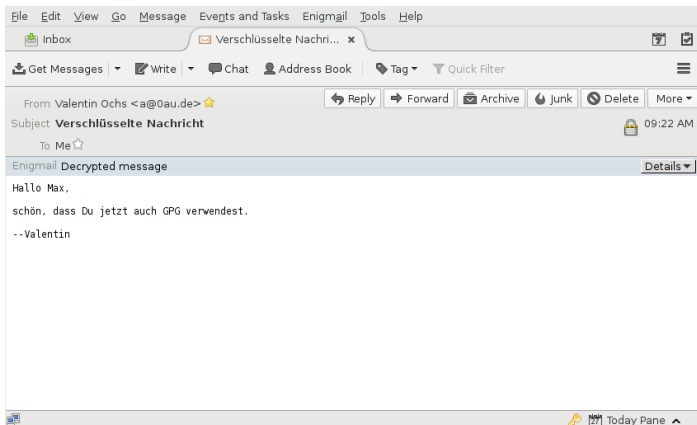
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



# Anzeige einer entschlüsselten Nachricht (1/3)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

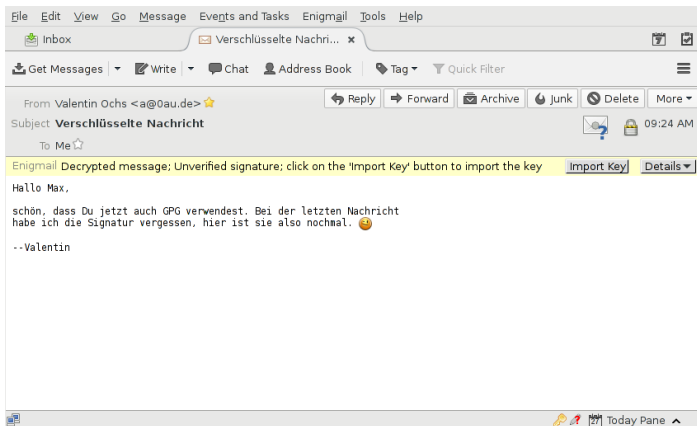
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



# Anzeige einer entschlüsselten Nachricht (2/3)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

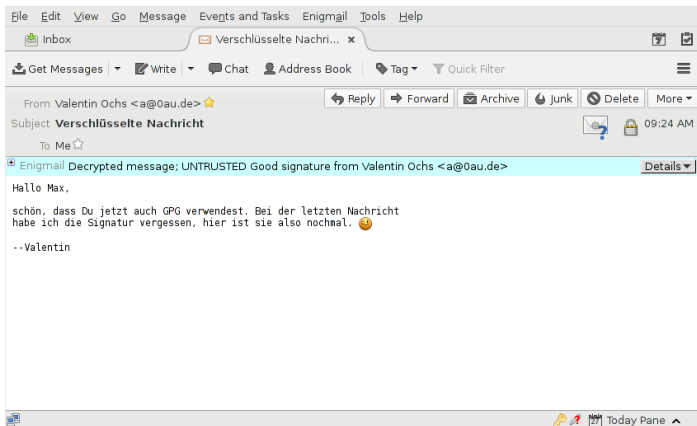
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



# Anzeige einer entschlüsselten Nachricht (3/3)

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

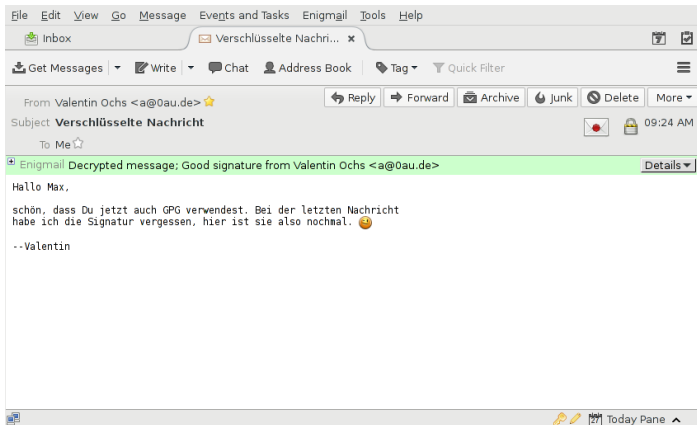
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



# Anzeige einer signierten Nachricht

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

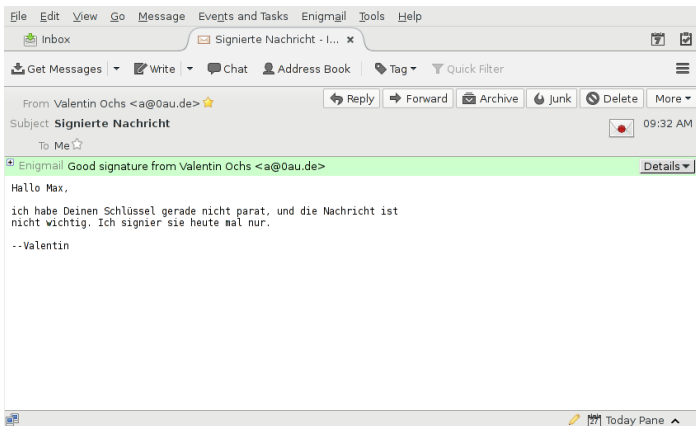
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



# Anzeige einer gefälschten Nachricht

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

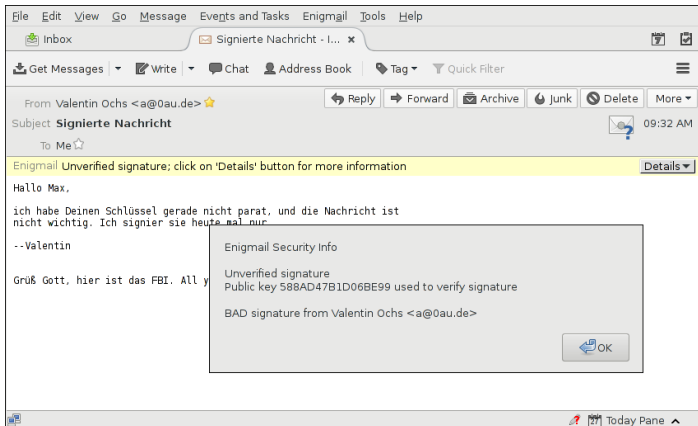
Grundlagen

Enigmail

Schlüsselver-  
waltung

Nachrichten  
senden und  
empfangen

Ende



- 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

Creative Commons Attribution-ShareAlike, unter <https://creativecommons.org/licenses/by-sa/2.0/> zu finden.

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



# Kontakt

E-Mail Ver-  
schlüsselung  
mit Enigmail

Valentin  
Ochs  
a@0au.de

Grundlagen

Enigmail  
Schlüsselver-  
waltung  
Nachrichten  
senden und  
empfangen

Ende

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