

# E-Mail Verschlüsselung mit GPG

Daniel Schulte

15. Januar 2014

- 1 Was ist GPG?
- 2 Warum sollte ich GPG verwenden?
- 3 Kurzübersicht: Wie funktioniert GPG?
- 4 GPG verwenden

- 1 Was ist GPG?
- 2 Warum sollte ich GPG verwenden?
- 3 Kurzüberblick: Wie funktioniert GPG?
- 4 GPG verwenden

# Was ist GPG?

## Geschichte, PGP

- PGP (engl. abk. „Pretty Good Privacy“) wurde 1991 von Phil Zimmermann veröffentlicht

# Was ist GPG?

## Geschichte, PGP

- PGP (engl. abk. „Pretty Good Privacy“) wurde 1991 von Phil Zimmermann veröffentlicht
- Ziel war es jedem sichere, elektronische Kommunikation zu ermöglichen

# Was ist GPG?

## Geschichte, PGP

- PGP (engl. abk. „Pretty Good Privacy“) wurde 1991 von Phil Zimmermann veröffentlicht
- Ziel war es jedem sichere, elektronische Kommunikation zu ermöglichen
- Da kryptographische Algorithmen in den USA unter Exportbeschränkungen fielen, gab es erst nur Versionen mit „schwacher“ Kryptographie außerhalb der USA

# Was ist GPG?

## Geschichte, PGP

- PGP (engl. abk. „Pretty Good Privacy“) wurde 1991 von Phil Zimmermann veröffentlicht
- Ziel war es jedem sichere, elektronische Kommunikation zu ermöglichen
- Da kryptographische Algorithmen in den USA unter Exportbeschränkungen fielen, gab es erst nur Versionen mit „schwacher“ Kryptographie außerhalb der USA
- Der Source Code wurde dann 1995 als Buch „PGP Source Code and Internals“ aus den USA exportiert und von freiwilligen abgetippt und als PGPi veröffentlicht

# Was ist GPG?

## Geschichte, PGP

- PGP (engl. abk. „Pretty Good Privacy“) wurde 1991 von Phil Zimmermann veröffentlicht
- Ziel war es jedem sichere, elektronische Kommunikation zu ermöglichen
- Da kryptographische Algorithmen in den USA unter Exportbeschränkungen fielen, gab es erst nur Versionen mit „schwacher“ Kryptographie außerhalb der USA
- Der Source Code wurde dann 1995 als Buch „PGP Source Code and Internals“ aus den USA exportiert und von freiwilligen abgetippt und als PGPi veröffentlicht
- PGP ist (auch heute noch) Closed Source und gehört momentan der Firma Symantec



# Was ist GPG?

Geschichte, GPG

- GPG steht für „GNU Privacy Guard“

# Was ist GPG?

Geschichte, GPG

- GPG steht für „GNU Privacy Guard“
- GPG implementiert den OpenPGP Standard nach RFC4880

# Was ist GPG?

## Geschichte, GPG

- GPG steht für „GNU Privacy Guard“
- GPG implementiert den OpenPGP Standard nach RFC4880
- GPG wurde erstmals 1999 veröffentlicht

# Was ist GPG?

## Geschichte, GPG

- GPG steht für „GNU Privacy Guard“
- GPG implementiert den OpenPGP Standard nach RFC4880
- GPG wurde erstmals 1999 veröffentlicht
- Es wurde als alternative zu PGP entwickelt

# Was ist GPG?

## Geschichte, GPG

- GPG steht für „GNU Privacy Guard“
- GPG implementiert den OpenPGP Standard nach RFC4880
- GPG wurde erstmals 1999 veröffentlicht
- Es wurde als alternative zu PGP entwickelt
- Es ist Open Source

- 1 Was ist GPG?
- 2 Warum sollte ich GPG verwenden?
- 3 Kurzüberblick: Wie funktioniert GPG?
- 4 GPG verwenden

# Warum GPG verwenden?

- Es kann deine Mails vor neugierigen Menschen (oder Serverbetreibern) schützen

# Warum GPG verwenden?

- Es kann deine Mails vor neugierigen Menschen (oder Serverbetreibern) schützen
- Es gibt dir die Möglichkeit sicher zu gehen das an der Mail unterwegs niemand „Fehler korrigiert“ hat



# Warum GPG verwenden?

- Es kann deine Mails vor neugierigen Menschen (oder Serverbetreibern) schützen
- Es gibt dir die Möglichkeit sicher zu gehen das an der Mail unterwegs niemand „Fehler korrigiert“ hat
- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschrieben zu haben

# Warum GPG verwenden?

- Es kann deine Mails vor neugierigen Menschen (oder Serverbetreibern) schützen
- Es gibt dir die Möglichkeit sicher zu gehen das an der Mail unterwegs niemand „Fehler korrigiert“ hat
- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschrieben zu haben
- Du musst jemand nicht unbedingt direkt kennen um ihm zu Vertrauen (Web of Trust)

# Warum GPG verwenden?

- Es kann deine Mails vor neugierigen Menschen (oder Serverbetreibern) schützen
- Es gibt dir die Möglichkeit sicher zu gehen das an der Mail unterwegs niemand „Fehler korrigiert“ hat
- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschrieben zu haben
- Du musst jemand nicht unbedingt direkt kennen um ihm zu Vertrauen (Web of Trust)
- GPG ist „starke“ Kryptographie

- 1 Was ist GPG?
- 2 Warum sollte ich GPG verwenden?
- 3 Kurzüberblick: Wie funktioniert GPG?**
- 4 GPG verwenden

# Wie funktioniert GPG?

## Hintergrund

- GPG und PGP arbeiten nach dem Prinzip des Public-Key-Kryptosystem oder asymmetrischen Kryptosystems

# Wie funktioniert GPG?

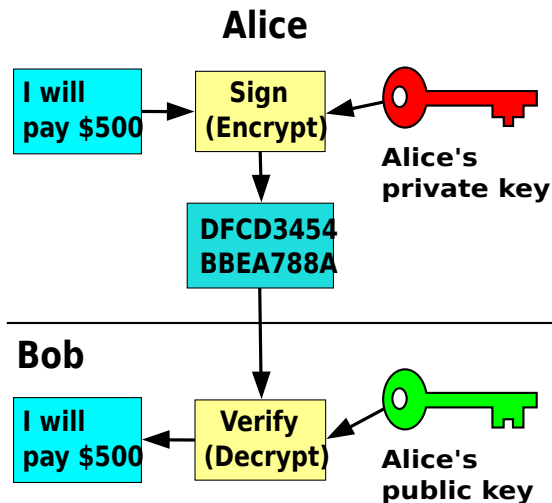
## Hintergrund

- GPG und PGP arbeiten nach dem Prinzip des Public-Key-Kryptosystem oder asymmetrischen Kryptosystems
- Den *geheimen/privaten* Teil darf niemand außer dir kennen, den *öffentlichen* Teil, sollen möglichst viele Leute kennen

# Wie funktioniert GPG?

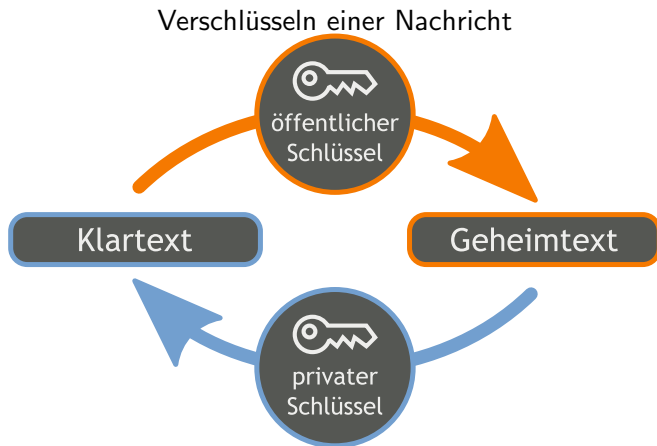
## Beispiel

Signieren einer Nachricht



# Wie funktioniert GPG?

Beispiel





- 1 Was ist GPG?
- 2 Warum sollte ich GPG verwenden?
- 3 Kurzüberblick: Wie funktioniert GPG?
- 4 GPG verwenden

- Ihr könnt GPG sowohl auf der Kommandozeile als auch aus eurem Mailprogramm heraus bedienen

- Ihr könnt GPG sowohl auf der Kommandozeile als auch aus eurem Mailprogramm heraus bedienen
- Ich zeige euch die Bedienung von GPG in Thunderbird

- Ihr könnt GPG sowohl auf der Kommandozeile als auch aus eurem Mailprogramm heraus bedienen
- Ich zeige euch die Bedienung von GPG in Thunderbird
- Wie ihr GPG von der Kommandozeile aus bedient findet ihr auf dem Handout

- Einfache, öffentliche Möglichkeit Schlüssel auszutauschen

- Einfache, öffentliche Möglichkeit Schlüssel auszutauschen
- Es kann von jedem *anonym* gelesen und geschrieben werden

- Einfache, öffentliche Möglichkeit Schlüssel auszutauschen
- Es kann von jedem *anonym* gelesen und geschrieben werden
- Bevor ihr euren Schlüssel auf einen Keyserver hochladet solltet ihr ein *Revocation-Zertifikat* erstellen um den Schlüssel im Notfall als ungültig zu markieren

- Einfache, öffentliche Möglichkeit Schlüssel auszutauschen
- Es kann von jedem *anonym* gelesen und geschrieben werden
- Bevor ihr euren Schlüssel auf einen Keyserver hochladet solltet ihr ein *Revocation-Zertifikat* erstellen um den Schlüssel im Notfall als ungültig zu markieren
- Ein bekannter Keyserver-Pool mit über 3 Millionen gespeicherten Schlüssel ist der SKS-Pool (<http://sks-keyservers.net/>)



# Key-Signing

Worauf man achten sollte

- Wenn ihr euren PGP-Key unterschreiben lassen wollt muss euer Gegenüber eure *Key-ID* kennen

# Key-Signing

## Worauf man achten sollte

- Wenn ihr euren PGP-Key unterschreiben lassen wollt muss euer Gegenüber euere *Key-ID* kennen
- Es bietet sich an vor einer Key-Signing-Party einen *Keyslip* erstellt auf dem eure Key-ID und euer Fingerprint und ggf. auch euer Name steht

# Key-Signing

## Worauf man achten sollte

- Wenn ihr euren PGP-Key unterschreiben lassen wollt muss euer Gegenüber eure *Key-ID* kennen
- Es bietet sich an vor einer Key-Signing-Party einen *Keyslip* erstellt auf dem eure Key-ID und euer Fingerprint und ggf. auch euer Name steht
- Je nachdem wie gut ihr euer Gegenüber kennt, lasst euch einen (Amtlichen) Lichtbildausweis zeigen

# Key-Signing

## Worauf man achten sollte

- Wenn ihr euren PGP-Key unterschreiben lassen wollt muss euer Gegenüber euere *Key-ID* kennen
- Es bietet sich an vor einer Key-Signing-Party einen *Keyslip* erstellt auf dem eure Key-ID und euer Fingerprint und ggf. auch euer Name steht
- Je nachdem wie gut ihr euer Gegenüber kennt, lasst euch einen (Amtlichen) Lichtbildausweis zeigen
- Lest euch gegenseitig den *Fingerprint* des zu prüfenden Schlüssels vor und vergleicht ihn

# Key-Signing

## Worauf man achten sollte

- Wenn ihr euren PGP-Key unterschreiben lassen wollt muss euer Gegenüber eure *Key-ID* kennen
- Es bietet sich an vor einer Key-Signing-Party einen *Keyslip* erstellt auf dem eure Key-ID und euer Fingerprint und ggf. auch euer Name steht
- Je nachdem wie gut ihr euer Gegenüber kennt, lasst euch einen (Amtlichen) Lichtbildausweis zeigen
- Lest euch gegenseitig den *Fingerprint* des zu prüfenden Schlüssels vor und vergleicht ihn
- Danach (evtl. Zu Hause) ladet ihr den Schlüssel vom Keyserver, unterschreibt ihn und ladet ihn wieder auf den Keyserver oder versendet ihn per E-Mail

# GPG verwenden

## Installation von Enigmail in Thunderbird

- GPG wird von Thunderbird mittels der Erweiterung *Enigmail* unterstützt

# GPG verwenden

## Installation von Enigmail in Thunderbird

- GPG wird von Thunderbird mittels der Erweiterung *Enigmail* unterstützt
- Unter Linux ist GPG meistens schon vorinstalliert. Enigmail installiert ihr am besten über Paketverwaltung eurer Distribution

# GPG verwenden

## Installation von Enigmail in Thunderbird

- GPG wird von Thunderbird mittels der Erweiterung *Enigmail* unterstützt
- Unter Linux ist GPG meistens schon vorinstalliert. Enigmail installiert ihr am besten über Paketverwaltung eurer Distribution
- Unter Windows gibt es das gpg4win-Projekt ([gpg4win.org](http://gpg4win.org)) das alles nötige enthält. Dort installiert ihr Enigmail über die Addon-Verwaltung von Thunderbird



# GPG verwenden

## Installation von Enigmail in Thunderbird

- GPG wird von Thunderbird mittels der Erweiterung *Enigmail* unterstützt
- Unter Linux ist GPG meistens schon vorinstalliert. Enigmail installiert ihr am besten über Paketverwaltung eurer Distribution
- Unter Windows gibt es das gpg4win-Projekt ([gpg4win.org](http://gpg4win.org)) das alles nötige enthält. Dort installiert ihr Enigmail über die Addon-Verwaltung von Thunderbird
- Unter MacOS gibt es gpgtools ([gpgtools.org](http://gpgtools.org)) dies bietet standardmäßig Unterstützung für Mail.app. Solltet ihr Thunderbird nutzen wird auch hier Enigmail aus der Addon-Verwaltung installiert

# GPG verwenden

## Installation von Enigmail in Thunderbird

- GPG wird von Thunderbird mittels der Erweiterung *Enigmail* unterstützt
- Unter Linux ist GPG meistens schon vorinstalliert. Enigmail installiert ihr am besten über Paketverwaltung eurer Distribution
- Unter Windows gibt es das gpg4win-Projekt ([gpg4win.org](http://gpg4win.org)) das alles nötige enthält. Dort installiert ihr Enigmail über die Addon-Verwaltung von Thunderbird
- Unter MacOS gibt es gpgtools ([gpgtools.org](http://gpgtools.org)) dies bietet standardmäßig Unterstützung für Mail.app. Solltet ihr Thunderbird nutzen wird auch hier Enigmail aus der Addon-Verwaltung installiert
- In Thunderbird findest du dann in der Menüleiste einen Punkt „OpenPGP“ in dem du die Einstellungen und Funktionen von GPG findet

# Danke für die Aufmerksamkeit.

Noch Fragen?

E-Mail: [daniel.schulte@rwth-aachen.de](mailto:daniel.schulte@rwth-aachen.de)

Jabber: [trilader@shin-project.org](mailto:trilader@shin-project.org)