

Was ist PGP/GPG?

Und will ich das überhaupt?

Daniel Schulte

18. Oktober 2012

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

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

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 kryptografische Algorithmen in den USA unter Exportbeschränkungen fielen, gab es erst nur Versionen mit „schwacher“ Kryptografie 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 kryptografische Algorithmen in den USA unter Exportbeschränkungen fielen, gab es erst nur Versionen mit „schwacher“ Kryptografie 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 kryptografische Algorithmen in den USA unter Exportbeschränkungen fielen, gab es erst nur Versionen mit „schwacher“ Kryptografie 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 Das ist doof...

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. Yay!

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

Warum GPG verwenden?

- Freie Software veröffentlicht unter der GPLv2

Warum GPG verwenden?

- Freie Software veröffentlicht unter der GPLv2
- Es schützt deine Mails vor neugierigen Menschen

Warum GPG verwenden?

- Freie Software veröffentlicht unter der GPLv2
- Es schützt deine Mails vor neugierigen Menschen
- Es gibt dir die Möglichkeit sicher zu gehen das an der Mail unterwegs niemand „Fehler korrigiert“ hat

Warum GPG verwenden?

- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschieben zu haben

Warum GPG verwenden?

- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschieben zu haben
- Du musst jemand nicht unbedingt direkt kennen um ihm zu Vertrauen (Web of Trust)

Warum GPG verwenden?

- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschieben zu haben
- Du musst jemand nicht unbedingt direkt kennen um ihm zu Vertrauen (Web of Trust)
- GPG ist „starke“ Kryptografie

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

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
- Es gibt einen Privaten (Geheimen) und einen Öffentlichen Schlüssel

Wie funktioniert GPG?

Hintergrund

- GPG und PGP arbeiten nach dem Prinzip des Public-Key-Kryptosystem oder asymmetrischen Kryptosystems
- Es gibt einen Privaten (Geheimen) und einen Öffentlichen Schlüssel
- Basiert auf der Funktionsweise von mathematischen „Einwegfunktionen“

Wie funktioniert GPG?

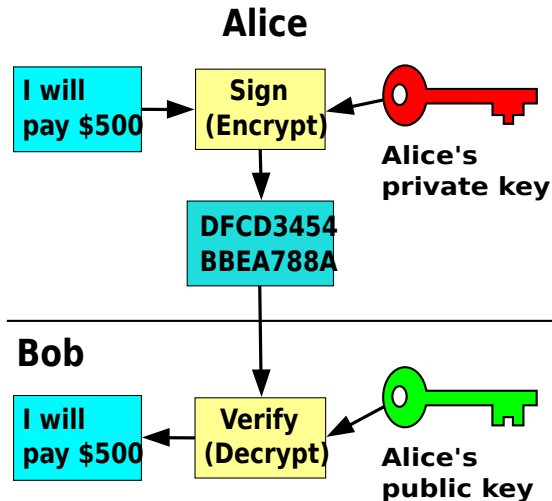
Hintergrund

- GPG und PGP arbeiten nach dem Prinzip des Public-Key-Kryptosystem oder asymmetrischen Kryptosystems
- Es gibt einen Privaten (Geheimen) und einen Öffentlichen Schlüssel
- Basiert auf der Funktionsweise von mathematischen „Einwegfunktionen“
- Wenn man den Schlüssel hat sind die Berechnungen vergleichsweise einfach, ohne Schlüssel dauern sie hingegen sehr lange (Primfaktorzerlegung)

Wie funktioniert GPG?

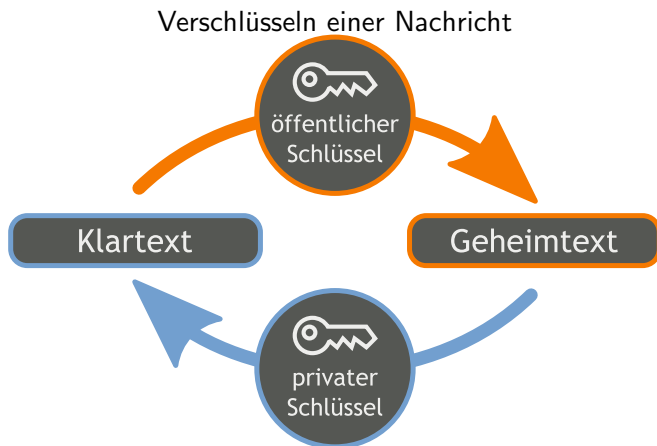
Beispiel

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**
- 5 GPG mit Thunderbird

GPG verwenden

Erstellen eines Schlüsselpaares

- Mit `gpg --gen-key` auf der Konsole könnt ihr ein neues Schlüsselpaar erzeugen.

GPG verwenden

Erstellen eines Schlüsselpaares

- Mit `gpg --gen-key` auf der Konsole könnt ihr ein neues Schlüsselpaar erzeugen.
- Ihr werdet einige Dinge gefragt, insbesondere solltet ihr eine sichere Passphrase wählen und euch diese sehr gut merken.

GPG verwenden

Erstellen eines Schlüsselpaares

- Mit `gpg --gen-key` auf der Konsole könnt ihr ein neues Schlüsselpaar erzeugen.
- Ihr werdet einige Dinge gefragt, insbesondere solltet ihr eine sichere Passphrase wählen und euch diese sehr gut merken.
- Mit `gpg --gen-revoke <key_id>` könnt ihr ein Wiederrufzertifikat für euren Schlüssel erstellen. Dies ist wichtig, solltet ihr den Key nicht mehr Benutzen oder sollte der private Teil des Schlüssels kompromittiert werden

GPG verwenden

Erstellen eines Schlüsselpaares

- Mit `gpg --gen-key` auf der Konsole könnt ihr ein neues Schlüsselpaar erzeugen.
- Ihr werdet einige Dinge gefragt, insbesondere solltet ihr eine sichere Passphrase wählen und euch diese sehr gut merken.
- Mit `gpg --gen-revoke <key_id>` könnt ihr ein Wiederrufzertifikat für euren Schlüssel erstellen. Dies ist wichtig, solltet ihr den Key nicht mehr Benutzen oder sollte der private Teil des Schlüssels kompromittiert werden
- Mittels `gpg --keyserver <server> --send-keys <key_id>` könnt ihr euren Schlüssel (oder den von anderen) auf einem Keyserver veröffentlichen

GPG verwenden

Unterschreiben von andern Schlüsseln

- Mit `gpg --keyserver <server> --search-keys <name>` könnt ihr nach Schlüsseln von anderen auf einem Keyserver suchen

GPG verwenden

Unterschreiben von andern Schlüsseln

- Mit `gpg --keyserver <server> --search-keys <name>` könnt ihr nach Schlüsseln von anderen auf einem Keyserver suchen
- Mit `gpg --recv-keys <key_id>` könnt ihr Schlüssel herunterladen

GPG verwenden

Unterschreiben von andern Schlüsseln

- Mit `gpg --keyserver <server> --search-keys <name>` könnt ihr nach Schlüsseln von anderen auf einem Keyserver suchen
- Mit `gpg --recv-keys <key_id>` könnt ihr Schlüssel herunterladen
- Mit `gpg --sign-key <key_id>` könnt ihr Schlüssel unterschreiben

GPG verwenden

Unterschreiben von andern Schlüsseln

- Mit `gpg --keyserver <server> --search-keys <name>` könnt ihr nach Schlüsseln von anderen auf einem Keyserver suchen
- Mit `gpg --recv-keys <key_id>` könnt ihr Schlüssel herunterladen
- Mit `gpg --sign-key <key_id>` könnt ihr Schlüssel unterschreiben
- Ein Beispiel für einen beliebten Keyserver ist `pool.sks-keyservers.net`

GPG verwenden

Ver- und Entschlüsseln

- Mit `gpg --encrypt --recipient <email> <filename>` könnt ihr Dateien verschlüsseln

GPG verwenden

Ver- und Entschlüsseln

- Mit `gpg --encrypt --recipient <email> <filename>` könnt ihr Dateien verschlüsseln
- Mit `gpg --output <decrypted_file> --dectypt <encrypted_file>` könnt ihr für euch verschlüsselte Dateien entschlüsseln

GPG verwenden

Signieren und Überprüfen von Signaturen

- Mit `gpg --sign --detach-sign <filename>` könnt ihr Dateien unterschreiben und die Unterschrift außerhalb der Datei als `filename.sig` ablegen. Dies ist wichtig bei Dateien die allergisch auf Veränderungen sind (Binärdaten)

GPG verwenden

Signieren und Überprüfen von Signaturen

- Mit `gpg --sign --detach-sign <filename>` könnt ihr Dateien unterschreiben und die Unterschrift außerhalb der Datei als `filename.sig` ablegen. Dies ist wichtig bei Dateien die allergisch auf Veränderungen sind (Binärdaten)
- Mit `gpg --verify <filename.sig>` könnt ihr, wenn ihr sowohl die Datei, als auch die Signatur Datei habt, die Signatur überprüfen

GPG verwenden

Signieren und Überprüfen von Signaturen

- Mit `gpg --sign --detach-sign <filename>` könnt ihr Dateien unterschreiben und die Unterschrift außerhalb der Datei als `filename.sig` ablegen. Dies ist wichtig bei Dateien die allergisch auf Veränderungen sind (Binärdaten)
- Mit `gpg --verify <filename.sig>` könnt ihr, wenn ihr sowohl die Datei, als auch die Signatur Datei habt, die Signatur überprüfen
- Solltet ihr eine Datei erhalten in der die Signatur integriert ist (d.h. sie wurde ohne `--detach-sign` erstellt) könnt ihr sie genau so verifizieren

GPG verwenden

Verwalten von User IDs (E-Mail-Adressen)

- Mit `gpg --edit-key <key_id>` könnt ihr euren Schlüssel interaktiv bearbeiten

GPG verwenden

Verwalten von User IDs (E-Mail-Adressen)

- Mit `gpg --edit-key <key_id>` könnt ihr euren Schlüssel interaktiv bearbeiten
- `gpg --edit-key <key_id> show` zeigt euch Informationen zu eurem Schlüssel an

GPG verwenden

Verwalten von User IDs (E-Mail-Adressen)

- Mit `gpg --edit-key <key_id>` könnt ihr euren Schlüssel interaktiv bearbeiten
- `gpg --edit-key <key_id> show` zeigt euch Informationen zu eurem Schlüssel an
- Mit `gpg --edit-key <key_id> adduid` könnt ihr eine User Id hinzufügen

GPG verwenden

Verwalten von User IDs (E-Mail-Adressen)

- Mit `gpg --edit-key <key_id>` könnt ihr euren Schlüssel interaktiv bearbeiten
- `gpg --edit-key <key_id> show` zeigt euch Informationen zu eurem Schlüssel an
- Mit `gpg --edit-key <key_id> adduid` könnt ihr eine User Id hinzufügen
- und mit `gpg --edit-key <key_id> revuid <nummer>` entfernen

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

- GPG/PGP wird in Thunderbird mit der Erweiterung Enigmail unterstützt

- GPG/PGP wird in Thunderbird mit der Erweiterung Enigmail unterstützt
- Hands On

Danke für die Aufmerksamkeit.

Noch Fragen?

E-Mail: daniel.schulte@rwth-aachen.de

Jabber: trilader@shin-project.org