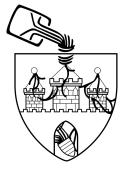
Sichere E-Mails mit PGP

Peter Gewald & Manuel Groß

2015-11-15

Wer sind wir?



https://ccc-ol.de/



https://mainframe.io/



CC-BY-SA 2.0 Markus Winkler



CC-BY-SA 2.0 Markus Winkler

• Massenhafte, anlasslose Überwachung



CC-BY-SA 2.0 Markus Winkler

- Massenhafte, anlasslose Überwachung
- False Positives



CC-BY-SA 2.0 Markus Winkler

- Massenhafte, anlasslose Überwachung
- False Positives
- Chilling Effect

Lösungsvorschlag: Verschlüsselung

----BEGIN PGP MESSAGE-----Version: GnuPG v2

hOTMA9vhUHWYLEX1A0/+07en6i6B00h91Ev02Zu/kEKXHW09GGNeXiPVtdGKMiUv FJwfZb7lL6hrpwNZJM8+iYWwKD7nv+nP4CHV5UlG0BLhMLMgPVM440TmR9APaiBf qUrUs8UzQ2syQCC52EUYGmwkRkjQofIVSsJj99TOwXt0M20zAdv1MQUH54HqFRRB Ou0g90437kPW8nBX226vWl./Sc6O0m2nvHmmkNrn+0B+sNimsVaWm+Cp5Y0p8k7vv aAdbuvRDddVVUK0zhNN+0PXiNolAzXU0eaBGnVhWL50aYZiCvat51HIRu+lURU0z nzdliZyssDis2rN/iVj8RcDWrpTmiKuKQAtKXIstLziYrQh6+2Nf37IztLjbIRkJ GkTuZSMAwJurlpDzWrik3t+sxXqF9drOxH1KSE9sM3EPZCYomdTdBVTep67iO0mI 5K8Txd04Tack8VHbVRd5IBJy8lVVnS8UyCdV5yjjx+KMxfZxUPlX9Ym0mB/jh06p d/eLU9TwomWNZtk7I8hVpVpmm8BvT+fbwTi33aUCcCDa8ic7vC6FsA3kiig7aDDL r3n0CR19LPibdvAMliHDddxOae4wbU2hN5aBFEiHBCOJPceI9euPrZmfzIMO3ou3 IP6cZBGLTawpHpz7NSzYBCAgKAXlQqXG2ptvVVL1Z96KhSxhZZ/LQc0MdySoYU0F AgwDvvGd00Bv5bYBD/0b5R7JBgt6aFN6MvnPr0XtlgEU4n9n+FRCvXVp03elCwlv ZGJ80iAa0SP00m0ECq+05Cs0JMPzmXq08Km7aKizY0nDv6ZAAD2VEbSfZkue0k03 bIbfbyeANOAlG80JTWsJSA2mPLXvD+E856jb6xVZpoAmrJjFfiSu2/awzw8giygH mVB+2vEUxcl8ollUdaPFketiEfWE00nAmYo2hT8WEqvviNNYT7pWll0NHU8kXZF3 j8ZyD377MNO4sR0il3f557L+e+zDJw6tCuDVQZjmeVihUijBlNNbwkZAC/+Dv8nS mJ9u9ZA9i2P0635SmZiseYWsphGhsI+2ngswtmvv2lYr9raX+PUYvG5nIAtD7CYr ge40nvHDFmFbIPrid6pzi+g6Gde0KCf0YJv+MlLtCi0INAsWFlvudT0crnR0ok0Z MXHval/Ez8XG0Mat4baZasVaOCL9CXanrx0WMG0h/dZaBZB0hkVGSXi/Fe5Bvlkz ggYCd5n5gJtT9e5RRELDGIBwaIJWV8TUXfhlOKBOsf5FT5zUr0ELSAzz+crkJkkh U+sloRzI471uNQoCbCehuv16sZ9niNlvrggtlcXvGVamZSMgH0lUxN6dNh+ASu9w pHorKveh70a/AGBc3ol.Zfo700B46oTtTXZb0xzB9tEHzxtC0TxCsl.r6HDcCoTNLt E982fPxAWcMSJyUIkiHx1NTYZdDXRóNqVQ14JA6YFmjf/vl/4dQGbNOvkhIyNqsB 8RgAgArhykdvd/+aD9Xdu0zGZ0d2tUg7p40mIi/vPi3/m5VaWiuUAUcdG0008bkW

- Klartext → Geheimtext
- mathematisches Verfahren
- geheime Zahl als "Passwort"

Lösungsvorschlag: Verschlüsselung

----BEGIN PGP MESSAGE-----Version: GnuPG v2

hOTMA9vhUHWYLEX1A0/+07en6i6B00h91Ev02Zu/kEKXHW09GGNeXiPVtdGKMiUv FJwfZb7lL6hrpwNZJM8+iYWwKD7nv+nP4CHV5UlG0BLhMLMqPVM440TmR9APaiBf qUrUs8UzQ2syQCC52EUYGmwkRkjQofIVSsJj99TOwXt0M20zAdv1MQUH54HqFRRB Ou0g90437kPW8nBX226vWl./Sc6O0m2nvHmmkNrn+0B+sNimsVaWm+Cp5Y0p8k7vv aAdbuvRDddVVUK0zhNN+0PXiNolAzXU0eaBGnVhWL50aYZiCvat51HIRu+lURU0z nzdliZyssDis2rN/iVj8RcDWrpTmiKuKQAtKXIstLziYrQh6+2Nf37IztLjbIRkJ GkTuZSMAwJurlpDzWrik3t+sxXqF9drOxH1KSE9sM3EPZCYomdTdBVTep67iO0mI 5K8Txd04Tack8VHbVRd5IBJy8lVVnS8UyCdV5yjjx+KMxfZxUPlX9Ym0mB/jh06p d/eLU9TwomWNZtk7I8hVpVpmm8BvT+fbwTi33aUCcCDa8ic7vC6FsA3kiig7aDDL r3n0CR19LPibdvAMliHDddxOae4wbU2hN5aBFEiHBCOJPceI9euPrZmfzIMO3ou3 IP6cZBGLTawpHpz7NSzYBCAgKAXlQqXG2ptvVVL1Z96KhSxhZZ/LQc0MdySoYU0F AgwDvvGd00Bv5bYBD/0b5R7JBgt6aFN6MvnPr0XtlgEU4n9n+FRCvXVp03elCwlv ZGJ80iAa0SP00m0ECq+05Cs0JMPzmXq08Km7aKizY0nDv6ZAAD2VEbSfZkue0k03 bIbfbyeANOAlG80JTWsJSA2mPLXvD+E856jb6xVZpoAmrJjFfiSu2/awzw8giygH mVB+2vEUxcl8ollUdaPFketiEfWE00nAmYo2hT8WEqvviNNYT7pWll0NHU8kXZF3 j8ZyD377MNO4sR0il3f557L+e+zDJw6tCuDVQZjmeVihUijBlNNbwkZAC/+Dv8nS mJ9u9ZA9i2P0635SmZiseYWsphGhsI+2ngswtmvv2lYr9raX+PUYvG5nIAtD7CYr ge40nvHDFmFbIPrid6pzi+g6Gde0KCf0YJv+MlLtCi0INAsWFlvudT0crnR0ok0Z MXHval/Ez8XG0Mat4baZasVaOCL9CXanrxQWMG0h/dZaBZB0hkVGSXi/Fe5Bvlkz ggYCd5n5gJtT9e5RRELDGIBwaIJWV8TUXfhlOKBOsf5FT5zUr0ELSAzz+crkJkkh U+sloRzI471uNQoCbCehuv16sZ9niNlvrggtlcXvGVamZSMgH0lUxN6dNh+ASu9w E982fPxAWcMSJyUIkiHx1NTYZdDXRóNqVQ14JA6YFmjf/vl/4dQGbNOvkhIyNqsB 8RgAgArhykdvd/+aD9Xdu0zGZ0d2tUg7p40mIi/vPi3/m5VaWiuUAUcdG0008bkW

- Klartext → Geheimtext
- mathematisches Verfahren
- geheime Zahl als "Passwort"
- symmetrisch
 - selbes Verfahren
 - selber Schlüssel

Lösungsvorschlag: Verschlüsselung

----BEGIN PGP MESSAGE-----Version: GnuPG v2

hOTMA9vhUHWYLEX1A0/+07en6i6B00h91Ev02Zu/kEKXHW09GGNeXiPVtdGKMiUv FJwfZb7lL6hrpwNZJM8+iYWwKD7nv+nP4CHV5UlG0BLhMLMqPVM440TmR9APaiBf qUrUs8UzQ2syQCC52EUYGmwkRkjQofIVSsJj99TOwXt0M20zAdv1MQUH54HqFRRB Ou0g90437kPW8nBX226vWl./Sc6O0m2nvHmmkNrn+0B+sNimsVaWm+Cp5Y0p8k7vv aAdbuvRDddVVUK0zhNN+0PXiNolAzXU0eaBGnVhWL50aYZiCvat51HIRu+lURU0z nzdliZyssDis2rN/iVj8RcDWrpTmiKuKQAtKXIstLziYrQh6+2Nf37IztLjbIRkJ GkTuZSMAwJurlpDzWrik3t+sxXqF9drOxH1KSE9sM3EPZCYomdTdBVTep67iO0mI 5K8Txd04Tack8VHbVRd5IBJy8lVVnS8UyCdV5yjjx+KMxfZxUP1X9Ym0mB/jh06p d/eLU9TwomWNZtk7I8hVpVpmm8BvT+fbwTi33aUCcCDa8ic7vC6FsA3kiig7aDDL r3n0CR19LPibdvAMliHDddxOae4wbU2hN5aBFEiHBCOJPceI9euPrZmfzIMO3ou3 IP6cZBGLTawpHpz7NSzYBCAgKAXlQqXG2ptvVVL1Z96KhSxhZZ/LQc0MdySoYU0F AgwDvvGd00Bv5bYBD/0b5R7JBgt6aFN6MvnPr0XtlgEU4n9n+FRCvXVp03elCwlv ZGJ80iAa0SP00m0ECq+05Cs0JMPzmXq08Km7aKizY0nDv6ZAAD2VEbSfZkue0k03 bIbfbyeANOAlG80JTWsJSA2mPLXvD+E856jb6xVZpoAmrJjFfiSu2/awzw8giygH mVB+2vEUxcl8ollUdaPFketiEfWE00nAmYo2hT8WEqvviNNYT7pWll0NHU8kXZF3 j8ZyD377MNO4sR0il3f557L+e+zDJw6tCuDVQZjmeVihUijBlNNbwkZAC/+Dv8nS mJ9u9ZA9i2P0635SmZiseYWsphGhsI+2ngswtmvv2lYr9raX+PUYvG5nIAtD7CYr ge40nvHDFmFbIPrid6pzi+g6Gde0KCf0YJv+MlLtCi0INAsWFlvudT0crnR0ok0Z MXHwql/Fz8XGQMqt4bqZosVqQCL9CXqmrxOWMGQh/dZqB7B0hkVGSXi/Fe5Rwlkz ggYCd5n5gJtT9e5RRELDGIBwaIJWV8TUXfhlOKBOsf5FT5zUr0ELSAzz+crkJkkh U+sloRzI471uNQoCbCehuv16sZ9niNlvrggtlcXvGVamZSMgH0lUxN6dNh+ASu9w E982fPxAWcMSJyUIkiHx1NTYZdDXRóNqVQ14JA6YFmjf/vl/4dQGbNOvkhIyNqsB 8RgAgArhykdvd/+aD9Xdu0zGZ0d2tUg7p40mIi/vPi3/m5VaWiuUAUcdG0008bkW

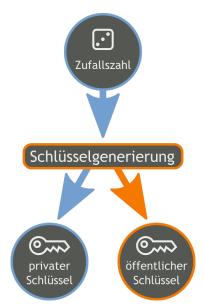
- Klartext → Geheimtext
- mathematisches Verfahren
- geheime Zahl als "Passwort"
- symmetrisch
 - selbes Verfahren
 - selber Schlüssel
- asymmetrisch
 - selbes Verfahren
 - unterschiedliche Schlüssel

Abgrenzung: Verschlüsselung

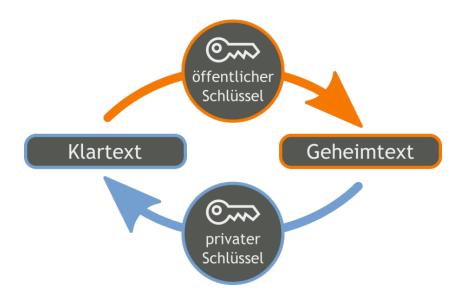
Was ist damit nicht gemeint?

- Transportverschlüsselung
 - ▶ SSL
 - ► TLS
 - → Nachrichten am Speicherort ungeschützt
- DE-Mail
 - per default nur abschnittweise verschlüsselt

Asymmetrische Verschlüsselung



Asymmetrische Verschlüsselung



Problem: Vertrauenswürdigkeit

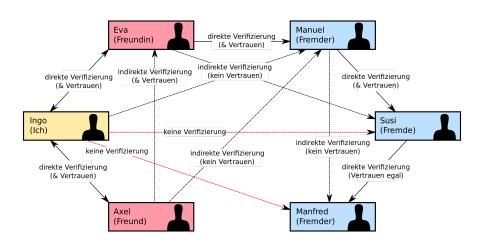
Problem:

Wer garantiert uns, dass Bob wirklich der Absender ist?

- Idee: zentraler Ansatz
 - Indirekter Austausch über Dritte (z.B. Browser oder Mailprogramm)
 - ► Hierarchie/Zertifikatsliste (schonmal reingeschaut?)



Unterschiedliche Ansätze: Verteilt



CC-BY-SA 3.0 Hauke Laging



CC-BY 2.0 wbritzl

```
pub rsa4096/63B7B190 2014-10-18
Key fingerprint = FF9A C23C EBC5 CD0D 3998 CB4A CB77 6720 63B7 B190
uid [ultimate] Manuel Groß <manuel.gross@freifeld-festival.de>
uid [ultimate] M:r:_el Groß <mgr@nordkrater.de>
```



CC-BY 2.0 wbritzl

Neue Leute kennenlernen



CC-BY 2.0 wbritzl

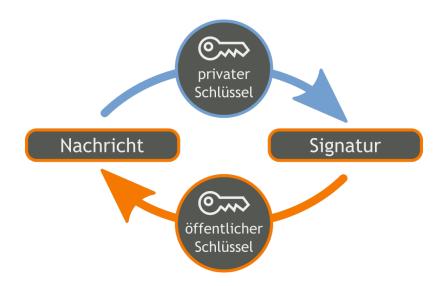
- Neue Leute kennenlernen
- Spaß an lustigen, alten, Ausweisbilder anderer haben



CC-BY 2.0 wbritzl

- Neue Leute kennenlernen
- Spaß an lustigen, alten, Ausweisbilder anderer haben
- ullet Selbst Cryptoparties veranstalten \Rightarrow Web of trust stärken

Signatur



GPG

Was ist jetzt eigentlich GPG?



- "Gnu Privacy Guard", Open Source-Implementierung von OpenPGP
- ,,PGP" (,,Pretty Good Privacy"), alternative, nun proprietäre Implementierung
- Sehr verbreitet im Open Source Umfeld

GPG

Was ist jetzt eigentlich GPG?



- "Gnu Privacy Guard", Open Source-Implementierung von OpenPGP
- "PGP" ("Pretty Good Privacy"), alternative, nun proprietäre Implementierung
- Sehr verbreitet im Open Source Umfeld
- Eher ungebräuchlich im geschäftlichen Umfeld
- Web of Trust Prinzip

GPG

Was ist jetzt eigentlich GPG?



- "Gnu Privacy Guard", Open Source-Implementierung von OpenPGP
- ,,PGP" (,,Pretty Good Privacy"), alternative, nun proprietäre Implementierung
- Sehr verbreitet im Open Source Umfeld
- Eher ungebräuchlich im geschäftlichen Umfeld
- Web of Trust Prinzip
- Plugins für viele Clients
- Metadaten nicht verschlüsselt!
- Teilweise Probleme mit Wrapping (z.B. Thunderbird)

PGP funktioniert!

TOP SECRET//COMINT//REL TO USA, AUS

TOP SECRET//COMINT//REL TO USA, AUS//20320108

THIS INFORMATION IS DERIVED FROM FAA
COLLECTION UNDER FAA COUNTERTERRORISM CERT

THIS INFORMATION IS PROVIDED FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL LEADS. IT CANNOT BE USED IN AFFIDAVITS, COURT PROCEEDINGS OR SUBPOENAS, OR FOR OTHER LEGAL OR JUDICIAL PURPOSES.

GPG unter Linux - Installation

Debian Pakete:

- gnupg2
- signing-party (für caff)
- msmtp

GPG unter Linux - Konfiguration

- Config: ∼/.gnupg/gpg.conf
- keyserver pgp.mit.edu
- Vorteil: Kein manuelles --keyserver <keyserver>

• \$ gpg --gen-key

- \$ gpg --gen-key
 - ► RSA oder DSA?

- \$ gpg --gen-key
 - ► RSA oder DSA?
 - ► Schlüssellänge?

- \$ gpg --gen-key
 - ► RSA oder DSA?
 - ► Schlüssellänge?
 - ► Gültigkeit?

- \$ gpg --gen-key
 - ► RSA oder DSA?
 - ► Schlüssellänge?
 - ► Gültigkeit?
 - ► Name (kein Pseudonym)

- \$ gpg --gen-key
 - ► RSA oder DSA?
 - ► Schlüssellänge?
 - ► Gültigkeit?
 - ► Name (kein Pseudonym)
 - ▶ Mailadresse

- \$ gpg --gen-key
 - ► RSA oder DSA?
 - ► Schlüssellänge?
 - ► Gültigkeit?
 - ► Name (kein Pseudonym)
 - Mailadresse
 - ▶ Passphrase (Langes_Passwort > S4I4t)

- \$ gpg --gen-key
 - ► RSA oder DSA?
 - ► Schlüssellänge?
 - ► Gültigkeit?
 - ▶ Name (kein Pseudonym)
 - Mailadresse
 - ▶ Passphrase (Langes_Passwort > S4I4t)
- Upload (sofern öffentlich):
 - \$ gpg --send-keys <key-id>

GPG unter Linux - Signieren

• Laden des fremden Keys:

\$ gpg --recv-keys <key-id>

GPG unter Linux - Signieren

- Laden des fremden Keys:
 - \$ gpg --recv-keys <key-id>
- Prüfung des Fingerprints:
 - \$ gpg --fingerprint <key-id>

GPG unter Linux - Signieren

- Laden des fremden Keys:
 - \$ gpg --recv-keys <key-id>
- Prüfung des Fingerprints:
 - \$ gpg --fingerprint <key-id>
- Identitätsprüfung (Personalausweis, Führerschein)

GPG unter Linux - Signieren

- Laden des fremden Keys:
 - \$ gpg --recv-keys <key-id>
- Prüfung des Fingerprints:
 - \$ gpg --fingerprint <key-id>
- Identitätsprüfung (Personalausweis, Führerschein)
- Signieren:
 - \$ gpg --sign-key <key-id>

GPG unter Linux - Signieren

- Laden des fremden Keys:
 - \$ gpg --recv-keys <key-id>
- Prüfung des Fingerprints:
 - \$ gpg --fingerprint <key-id>
- Identitätsprüfung (Personalausweis, Führerschein)
- Signieren:
 - \$ gpg --sign-key <key-id>
- Passphrase eingeben

GPG unter Linux - Signieren

- Laden des fremden Keys:
 - \$ gpg --recv-keys <key-id>
- Prüfung des Fingerprints:
 - \$ gpg --fingerprint <key-id>
- Identitätsprüfung (Personalausweis, Führerschein)
- Signieren:
 - \$ gpg --sign-key <key-id>
- Passphrase eingeben
- Upload-Varianten:
 - Unsicher Direkter Upload auf Keyserver
 Sicher Verschicken des signierten Keys per Mail an die signierten Mailadressen

GPG unter Linux - Signieren mit caff

- Automatisch:
 - \$ caff <key-id>

GPG unter Linux - Signieren mit caff

- Automatisch:
 - \$ caff <key-id>
- Benötigt konfigurierten SMTP-client
- Beispiel msmtp

GPG unter Linux - Signieren mit caff

- Automatisch:
 - \$ caff <key-id>
- Benötigt konfigurierten SMTP-client
- Beispiel msmtp
- Config: ∼/.msmtprc
 - ► host, port, user, passwort

• Datei signature.asc per Mail bekommen

- Datei signature.asc per Mail bekommen
- Signatur importieren:

```
gpg --import signatur.asc
```

- Datei signature.asc per Mail bekommen
- Signatur importieren:

```
gpg --import signatur.asc
```

• Signatur Uploaden:

gpg --send-keys <meine key-id>

- Datei signature.asc per Mail bekommen
- Signatur importieren:

```
gpg --import signatur.asc
```

Signatur Uploaden:

Done! Ready for GPG-Mails!

• Entweder automatisch (Gültigkeit) oder manuell

- Entweder automatisch (Gültigkeit) oder manuell
- Wichtig: **Vorher** Cross-signieren

- Entweder automatisch (Gültigkeit) oder manuell
- Wichtig: Vorher Cross-signieren
- Revoken ≠ Löschen

- Entweder automatisch (Gültigkeit) oder manuell
- Wichtig: Vorher Cross-signieren
- Revoken ≠ Löschen
- Widerrufszertifikat:

• Importieren, Uploaden

- Entweder automatisch (Gültigkeit) oder manuell
- Wichtig: Vorher Cross-signieren
- Revoken ≠ Löschen
- Widerrufszertifikat:

- Importieren, Uploaden
- ggf. direkt nach Generierung erzeugen
- Besser: Backup private key!

Hands-on - Let's go!

- Schlüsselpaar erstellen
 - ▶ gpg --gen-key
 - ► (keyserver definieren)
 - ▶ gpg --send-keys <key-id>
- Signieren mit Identitätsprüfung (z.B. ohne caff)
 - ▶ gpg --recv-keys <key-id>
 - ▶ gpg --fingerprint <key-id>
 - ▶ gpg --sign-key <key-id>
- Signaturen per Mail verschicken
 - ▶ caff <key-id>
- Uploaden auf den Keyserver (Empfänger)
 - ▶ gpg --import signatur.asc
 - ▶ gpg --send-keys <meine key-id>