PGP Hands-On:

Client Installation, Key Signing und ein paar nette Tricks

http://www.franken.de/kongress/pgp/PGP.pdf

Matthias Brüstle

Nürnberg 2014-11-23

Programm für die nächsten 3 Stunden:

- Installation von GnuPG (Linux / MS Windows)
- Konfiguration
- Schlüsselerzeugung (hier schon die Tricks)
- Thunderbird-Plugin EnigMail
- Party!

Software

- Debian-Pakete: gnupg2, gnupg-agent
- MS Windows http://www.gpg4win.org/download-de.html (http://www.franken.de/kongress/pgp/gpg4win-2.2.2.exe)
- gpg.conf:http://www.franken.de/kongress/pgp/gpg.conf
- Thunderbird: https://www.mozilla.org/de/thunderbird/
- EnigMail (Thunderbird-Add On)

gpg.conf (1)

```
### Mehr oder weniger von:
https://we.riseup.net/riseuplabs+paow/openpgp-best-practices
# Eindeutigere Ausgabe
fixed-list-mode
keyid-format 0xlong
with-fingerprint
verify-options show-uid-validity
list-options show-uid-validity
# Bevorzugte Algorithmen
personal-digest-preferences SHA512 SHA384 SHA256 SHA224
default-preference-list SHA512 SHA384 SHA256 SHA224 AES256 AES192
AES BZIP2 ZLIB ZIP Uncompressed
cert-digest-algo SHA512
# GnuPG-Agent
use-agent
#  Krücke
sig-notation issuer-fpr@notations.openpgp.fifthhorseman.net=%g
```

gpg.conf (2)

```
### Von mir
# Sorgfalt bei der Identitätsprüfung
ask-cert-level
default-cert-level 3
# Web of Trust
completes-needed 1
marginals-needed 3
max-cert-depth 5
# Nicht so viel Ausgabe
#quiet
no-greeting
# Keyserver
keyserver hkp://pool.sks-keyservers.net
# Standard-Schlüssel
#default-key 0x...
#default-recipient-self
#encrypt-to 0x...
#hidden-encrypt-to 0x...
# Geheimen Schlüssel auslagern
#secret-keyring /mnt/secring/secring.gpg
```

Web of Trust

- Zwei Fragen:
  - Gehört der Schlüssel der angegebenen Person? => validity
  - Vertraue ich der Person die Schlüssel anderer ordentlich zu prüfen und zu signieren? => trust (ultimate, complete, marginal, unknown)
- Konfigurationsparameter:
  - completes-needed 1
  - marginals-needed 3
  - max-cert-depth 5

GnuPG installieren

Nochmal zur Erinnerung:

- Debian-Pakete: gnupg2, gnupg-agent
- MS Windows http://www.gpg4win.org/download-de.html (http://www.franken.de/kongress/pgp/gpg4win-2.2.2.exe)

Wohin mit der gpg.conf?

- Linux: ~/.gnupg/
- Windows: C:\Users*USER*\AppData\Roaming\gnupg (gpg --version)

Schlüssel erzeugen

- Eckdaten:
  - 4096-bit RSA
  - kein Verfalldatum
  - Name und eMail-Adresse, kein Kommentar
- Kommandozeile: gpg(2) –gen-key
- GUI: Kleopatra

„Tricks“ mit gpg --edit-key

- addrevoker: Eintragen eines fremden Schlüssels, der den eigenen widerrufen kann
- expire
  - Ablaufdatum kann geändert/verlängert werden!
  - Für Verlängerungen am Einfachsten nur den Hauptschluessel verfallen zu lassen: Verfallsdatum nach der Erzeugung ergänzen
- Zusätzlichen Signatur-Unterschlüssel: https://alexcabal.com/creating-the-perfect-gpg-keypair/

EnigMail installieren

- Nochmal zur Erinnerung: https://www.mozilla.org/de/thunderbird/
- EnigMail (Thunderbird-Add On)
  - Einstellungen -> Senden -> Senden bestätigen: immer
  - Einstellungen -> Schlüsselserver -> „pgp.mit.edu“ entfernen

Problem: Schlüsselumzug

- Schlüssel widerrufen: gpg –edit-key -> revkey „Key is superseded“ + Kommentar
  - Niemand wird den Kommentar sehen
  - Keine damit erzeugte Signatur ist noch gültig (Signatur des neuen Schlüssels durch den alten)
- Nichts am alten Schlüssel tun
  - Schwieriger Leute vom Umzug zu informieren
  - Es gibt Software, die eMails einfach an alle passenden Empfängerschlüssel zu verschlüsseln

Lösung gesucht! (UserID ohne eMail hinzufügen, alte mit eMail widerrufen?)

Party!

- Normalerweise sammelt man die Fingerabdrücke vorab
- Vorschlag für heute:
  - Schlüsselinhaber kommen einzeln vor,
  - verlesen ihren Schlüsselfingerabdruck und
  - lassen ihr Ausweisdokument von ein paar Vertretern prüfen
  - Danach kann noch jeder mit jedem nach Bedarf

Saenks!

http://www.franken.de/kongress/pgp/PGP.pdf

Key fingerprint = EF9D F786 CBF1 1764 6BB4
CFA3 4569 E9B3 ECFF C9C9

Matthias Brüstle

Nürnberg 2014-11-24