GnuPG - sicherer E-Mail Verkehr

Norbert Tretkowski
Debian Entwickler
nobse@debian.org

Klassische Kryptographie Programme

- Kommunikationspartner müssen vor der Kommunikation geheime Schlüssel austauschen

- Lästig wenn sie sehr weit auseinander leben

Abhilfe

- Whitfield Diffie und Martin Hellmann entwickelten 1976 das asymetrische Verfahren
- Bei diesem hat jeder Benutzer zwei Schlüssel
  - einen öffentlichen (den er verbreitet)
  - einen privaten (der geheim bleiben muss)

Wie’s funktioniert

- Jemand will mir eine verschlüsselte E-Mail schicken
- Diese Person holt sich meinen öffentlichen Schlüssel von einem Keyserver
- Nachricht wird mit dem eben geholten Key verschlüsselt
- Nur der Besitzer des entsprechenden privaten Keys kann die Nachricht entschlüsseln

Populärste Implementation

Bisher PGP, aber

- Problem: CAF
- Source Code nicht verfügbar

Abhilfe: GnuPG

Anlegen eines neuen Keys (1)

- Aufruf: ‘gpg --gen-key‘
- Standardeinstellungen übernehmen
  - Algorithmus
  - Schlüssellänge
  - Gültigkeitsdauer

Anlegen eines neuen Keys (2)

- User-ID für den Schlüssel wählen
  - Name, z.B. ’Norbert Tretkowski’
  - Kommentar, z.B. ’nobse’
  - E-Mail Adresse, z.B. ’nobse@debian.org’

Anlegen eines neuen Keys (3)

- Passphrase eingeben
  - Der private Schlüssel wird nicht im Klartext gespeichert
  - Wird nur bei Bedarf entschlüsselt
  - Passphrase darf niemals über eine unsichere Verbindung eingegeben werden
- Nach Eingabe der Passphrase wird Schlüsselpaar generiert

Hinzufügen zusätzlicher User-ID’s

- Hinzufügen weiterer E-Mail Adressen möglich
- Befehl ’adduid’ auf der Schlüsselmanagement Console
- Erneute Abfrage von Name, Kommentar und E-Mail Adresse
- Löschen einer User-ID: ’deluid’

Revoke Zertifikat

- Revoke Zertifikat zum ungültig erklären eines Schlüssels
- Aufruf: ’gpg --gen-revoke <User-ID>
- Zertifikat wird ausgegeben
  - Speichern des Zertifikats auf einer Floppy
  - Ausdrucken des Zertifikats

Keys auf einen Keyserver

- Uploaden des Keys

  $ gpg --keyserver keys.de.pgp.net --send-key <User-ID>
  gpg: success sending to ‘keys.de.pgp.net’ (status=200)

- Aktualisieren des Keys durch erneutes Uploaden

- Loeschen eines Keys nicht moeglich

- Holen eines Keys

  $ gpg --keyserver keys.de.pgp.net --recv-key <User-ID>

Verschlüsseln und entschlüsseln

- Verschluesseln einer Datei
  $ gpg -a -r <User-ID oder Key-ID> -e <Dateiname>
- Neu Datei <Dateiname.asc>
- Entschluesseln via
  $ gpg -d <Dateiname>

Signieren und Prüfen

- Signieren einer Datei

  $ gpg -clearsign [-u <User-ID>] <Dateiname>

- Pruefen einer Signatur

  $ gpg -verify <Dateiname>

- Pruefen und ausgeben

  $ gpg -d <Dateiname>

Unterschreiben von Schlüsseln

- Nur bei
  - Vorlage des Fingerprints
  - Vorlage des Personalausweis oder Reisepass
- Importieren des Schlüssels
- Aufruf: ’gpg --sign-key <User-ID>’
- Key exportieren und an Besitzer schicken