4.2) E-Mail-Verschlüsselung

Praxis-Teil

Thunderbird, PGP/GPG, Enigmail

PGP vs. GPG

- **PGP**
  - **P**retty **G**ood **P**rivacy
  - das Original
  - kommerziell vermarktetes Programm
  - *Prinzip,* das heute jeder nutzt

- **GPG**
  - **G**NU **P**rivacy **G**uard
  - quelloffene und freie Weiterentwicklung
  - *Programm*, das heute jeder nutzt

Installation

Thunderbird, GPG

Linux	über die Paket-Suche installierbar `thunderbird`, `gnupg`
Windows	https://www.mozilla.org/de/thunderbird/ http://www.gpg4win.de/download-de.html
Mac OS	https://www.mozilla.org/de/thunderbird/ https://gpgtools.org/

CP#1

Installation

GPG und Mobilgeräte

iOS, Windows Phone

- oPenGP

Android

- Thunderbird → K9-Mail
- GPG → Android Privacy Guard (APG)
- Schlüsselgenerierung nicht auf dem Smartphone zu empfehlen
- Eigene Schlüssel und E-Mail-Adresse für Smartphone-Nutzung empfehlenswert

Installation
Enigmail

- Add-On für Thunderbird
- Menü: Add-Ons → Enigmail suchen & installieren
- Thunderbird neustarten

CP#2

Schlüssel-Generierung

mit Enigmail

- Menü: Enigmail → Schlüssel verwalten
- Erzeugen → Neues Schlüsselpaar

CP#3

Schlüssel-Generierung

mit Enigmail

- Benutzerkennung
  E-Mail-Adresse für die er genutzt werden soll
- Haken setzen
  „Schlüssel zum Unterschreiben verwenden“
- **sichere** Passphrase erstellen & eingeben
- Ablaufzeit: Benutzbarkeit vs. Komfort
- Erweitert
  Schlüssellänge: 4096 bit
  Algorithmus : RSA
- „Schlüsselpaar erzeugen“

CP#4

Konfiguration

- Menü: Einstellungen → Konto-Einstellungen
  → E-Mail-Konto wählen: OpenPGP-Sicherheit
  → OpenPGP-Unterstützung aktivieren
  → Standard-Einstellungen anpassen: PGP/MIME benutzen
- Composition & Adressing (links unter E-Mail-Adresse)
  Haken entfernen: „Nachrichten im HTML-Format versenden“
- Kopieren & Ordner
  → Entwürfe und Vorlagen lokal speichern/ „lokalen Ordnern“

CP#5

Allgemeines zu PGP-Schlüsseln

- Eindeutige Zuordnung von Schlüssel ←→ Besitzer
- Wenn kompromitiert: Gesamte Kommunikation lesbar

Lösung: OTR statt PGP … andere CP

Schlüsselverwaltung

Warum?

- Gegenseite braucht meinen öffentlichen Schlüssel, um eine Nachricht an mich zu verschlüsseln

- Backup von öffentlichem & privatem Schlüssel

Alle Schlüssel (meine & die Dritter) werden im Schlüsselbund a.k.a. keyring gespeichert.

Schlüsselverwaltung

Schlüsselaustausch

1) Bei jeder E-Mail im Anhang mitschicken (automatisch)

Menü: Bearbeiten → E-Mail-Einstellungen
→ Profil: OpenPGP-Sicherheit → Erweitert …
→ „Öffentlichen Schlüssel an Nachricht anhängen“

Schlüsselverwaltung
Schlüsselaustausch

2) Bei jeder E-Mail im Anhang mitschicken (manuell)

Menü: Enigmail → Schlüssel verwalten
→ Rechtsklick auf Schlüssel
→ „Öffentlichen Schlüssel per E-Mail senden“

Schlüssel erscheint unter „Anhänge“ als Datei
Bsp-Name: `0x345E641F.asc`

Schlüsselverwaltung
Schlüsselaustausch

3) Export auf Speichermedium

Menü: Enigmail → Schlüssel verwalten
→ Rechtsklick auf Schlüssel
→ „Exportieren“
→ Nachfrage mit „Nur öffentlichen Schlüssel exportieren” beantworten
→ Speicherort auswählen und bestätigen

Schlüsselverwaltung
Schlüsselaustausch

4) Import von Speichermedium

Menü: Enigmail → Schlüssel verwalten
→ Menu: Datei
→ „Importieren“
→ Schlüssel-Datei auswählen und bestätigen

funktioniert sowohl für öffentliche
als auch private Schlüssel

Schlüsselverwaltung
Authentifizierung

Grundsätzlich fremde öffentliche Schlüssel vor dem ersten Gebrauch authentifizieren (fingerprint).

- ID zu kurz, Gefahr von Kollisionen → fingerprint
- fingerprint über sicheren Kanal austauschen, z.B. telefonisch oder persönlich, und überprüfen
- Nur Schlüsseln vertrauen, die man überprüft hat.

miehl@w3hs.net
9939 7DD1 42F4 85BE 2507 ED29 94F8 9BD7 345E 641F

Schlüsselverwaltung

Schlüssel-Server a.k.a. keyserver

Geben einem die Möglichkeit den öffentlichen Schlüssel im Internet zu hinterlegen, damit er von Dritten zum Verschlüsseln genutzt werden kann.

Durchsuchbar nach

- Name
- E-Mail-Adresse
- IDs (kurz, lang)
- Fingerprint

Schlüsselverwaltung

Schlüssel-Server und Enigmail

- Erlaubt Konfiguration von Key-Servern
  zum automatischen Abgleich

- Menü:
  Enigmail → Einstellungen → Schlüsselserver
  → eintragen: „pool.sks-keyservers.net“

- Zur Signatur-Überprüfung eintragen:
  „https://sks-keyservers.net/sks-keyservers.netCA.pem“

Schlüsselverwaltung

Schlüssel-Server allgemein

- Wenn man sie nutzt, >1 benutzen (Server-Pools)
  → Weniger fehleranfällig als Einzelserver

- Empfehlung
  SKS Key-Server-Pool
  Infos unter https://sks-keyservers.net/

- Details von Einstellung GnuPG einstellen: gpg.conf
  https://help.riseup.net/en/security/message-security/openpgp/best-practices

Schlüsselverwaltung

Widerrufszertifikat erstellen

Sinnvoll im Zusammenhang mit der
Verwendung von Schlüssel-Servern.

Beispiele

1) Bei Verlust/ Kompromittierung des
   privaten Schlüssels für dessen Widerruf
2) Wenn der bisherige private Schlüssel überholt ist
   z.B. weil der neue stärker ist (mehr Bit, andere Standards)

WICHTIG: Backup des Widerrufszertifkats erstellen und
getrennt vom Arbeitsrechner speichern.

Vielen Dank fürs Feiern!

Selbststudium

http://www.cryptoparty.in/documentation

Spendenseiten

Chaotikum
https://www.betterplace.org/p18686/

SWU
https://www.betterplace.org/p24976/

Feedback an kontakt@swu-hl.de