IT Sicherheit

01 Übungen

OpenPGP – Web Of Trust

- GPG / GPG4Win installieren
- GPG/PGP Keypair und Zertifikat erzeugen
- Zertifikat mit anderen austauschen (Keyserver) und Zertifikate von anderen signieren (Vertrauen in Zertifikat sicherstellen)

- Nachricht erstellen und mit eigenem Private Key signieren
- Nachricht erstellen und mit Public Key von anderen verschlüsseln
- Nachricht erstellen, mit eigenen Private Key signieren, mit Public Key von KG (EE152F6FE34BAE542FEF66BBD1AD694E7EFA14CF) verschlüsseln und an KG per Email senden

X.509 – Hierarchische Zertifizierungsstellen

- Download Openssl.exe: https://www.heise.de/download/product/win32-openssl-47316
- PKI aufbauen
  - Config anlegen (Siehe openssl.conf) und einen **ca** und **ca\ca.db.certs** Ordner anlegen und leeres File (ca\ca.db.index) anlegen und ein File (ca\ca.db.serial) mit Inhalt 1000 anlegen
  - Root CA Private Key
    - `openssl genrsa -aes256 -out ca\myrootca.key 4096`
  - Root CA Zertifikat
    - `openssl req -x509 -new -nodes -key ca\myrootca.key -sha256 -days 3650 -out ca\myrootca.crt`
  - Zertifikat verifizieren
    - `openssl x509 -noout -text -in ca\myrootca.crt`
  - Intermediate Private Key
    - `openssl genrsa -aes256 -out ca\myintca.key 4096`
  - Intermediate Zertifikat Request
    - `openssl req -new -key ca\myintca.key -sha256 -out ca\myintca.csr`
  - CSR überprüfen
    - `openssl req -noout -text -in ca\myintca.csr`
  - Intermediate Zertifikat mit RootCA signieren
    - `openssl ca -config openssl.conf -extensions ca_signing_req -out ca\myintca.crt -infiles ca\myintca.csr`

X.509 – Hierarchische Zertifizierungsstellen

- Wird dem myintca.crt vertraut?
  - myrootca.crt in Zertifikatspeicher aufnehmen (Windows: User Store / Manuell den Root CA Store auswählen)
  - Wird dem myintca.crt jetzt vertraut? Wieso?

X.509 – Hierarchische Zertifizierungsstellen

- PKI verwenden
  - CSR erzeugen (Für die eigene IP Adresse als Common Name und als Subject Alternative Name – **gültig für 30 Tage**) und von anderem Intermediate Zertifikat signieren lassen
  - Andere Root CA in eigenen Zertifikat-Store aufnehmen
  - Überprüfen, ob Zertifikat vertraut wird – Troubleshooting

  - Einfachen Webserver laufen lassen (z.B. **openssl s_server**) und Zertifikat präsentieren – Können andere auf den Webserver zugreifen? Troubleshooting!

  - Andere Root CA wieder aus dem eigenen Zertifikat-Store entfernen

Freie CA - Let’s Encrypt / HTTP-01 Challenge

- Zertifikat von Let’s Encrypt für student<NR>.class5<a|b>hits.htl.gkcs.eu abholen
- Zertifikat auf Webserver einspielen
- Auf Domain mit passendem Port zugreifen und Zertifikat überprüfen
- Auf Domain mit anderer Nummer aber gleichem Port zugreifen und Zertifikat überprüfen