Vorbereitung

Bereits vor dem Praktikum sollten Sie sich anhand der im Internet verfügbaren Informationen über folgende Anwendungen informieren:

- openssl – Erzeugung von Benutzer-Zertifikaten
- apache – Konfiguration von SSL-Servern zur Kontrolle von Benutzer-Zertifikaten

Aufgabe 4a: Erzeugung von SSL-User-Zertifikaten

Auf Ihrem Server haben Sie für Aufgabe 2 bereits eine PKI zur Erzeugung von CA- und Server-Zertifikaten aufgebaut. Damit ist openssl verfügbar und auch eine grundlegende Struktur, die in diesem Aufgabenblatt erweitert werden soll.

Erweitern Sie Ihre PKI-Struktur so, dass Sie folgendes in einem geeigneten Format (das Ihr verwendete Client importieren kann) erzeugen können:

- ein SSL-User-Zertifikat für Ihre Gruppe XX, wobei XX durch Ihre Gruppennummer mit führender Null zu ersetzen ist:
  /C=DE; /O=haw-hamburg; /OU=informatik; \
  /CN=Team XX
  unterhalb der SSL-CA für die Organisationseinheit mit Namen:
  /C=DE; /O=haw-hamburg; /OU=informatik; /CN=CA

Überprüfen Sie, ob an der CRL-Erzeugung etwas ändern müssen und nehmen Sie entsprechend ggf. Änderungen vor!

Aufgabe 4b: Einrichten des SSL-User-Zertifikats

Richten Sie einen Browser wie Firefox oder Safari auf Ihrem Arbeitsplatzrechner so ein, dass das SSL-User-Zertifikat verwendet werden kann, um sich gegenüber Ihrem SSL-Server auszuweisen. Übertragen Sie das SSL-User-Zertifikat sicher dahin!

Aufgabe 4c: Einrichten des SSL-Servers für SSL-User-Zertifikate

Passen Sie die Konfiguration Ihres sicheren HTTPS-Apache-Server so an, dass ein Zugriff über HTTPS (443/tcp) auf „Ihre“ index-Seite möglich wird, allerdings nur, wenn Sie sich gegenüber dem Server mit Ihrem Browser und dem dort installierten SSL-User-Zertifikat (siehe Aufgabe 4b) erfolgreich identifizieren und authentisieren können.

Nach erfolgreicher Bearbeitung dieser Aufgabe haben Sie den größten Teil des Benutzermanagements von Ihrer Web-Anwendung in die PKI verlagert. Woran hängt jetzt die Sicherheit, wenn es keine Passworte mehr gibt und diese auch nicht vom Server geklaut werden können?