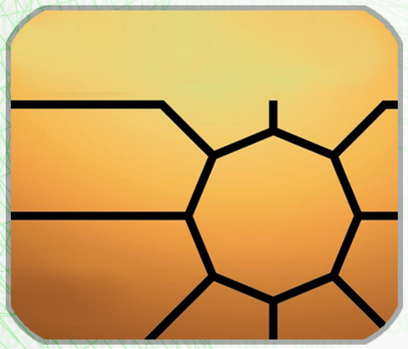
SMART CARD basierte Authentifizierung



Smart Card - Allgemein
Eine Smartcard oder auch Chipkarte ist eine Kunstoffkarte mit einem kleinen Computerchip der verschiedene Operationen ausführen kann. Mit der Hardware auf den Karten ist es möglich kryptographische Schüssel zu erzeugen und in dem Smartcardspeicher aufzubewahren.

Dieser Schlüsselspeicher kann nicht von außen gelesen werden. Um Zugriff auf die verfügbaren Operationen zu erlangen ist eine PIN (Personal Identification Number) und spezielle Smartcard-Lesegeräte erforderlich. Smartcards stellen eine äußerst sichere Umgebung für die Aufbewahrung geheimer Schlüssel bereit.

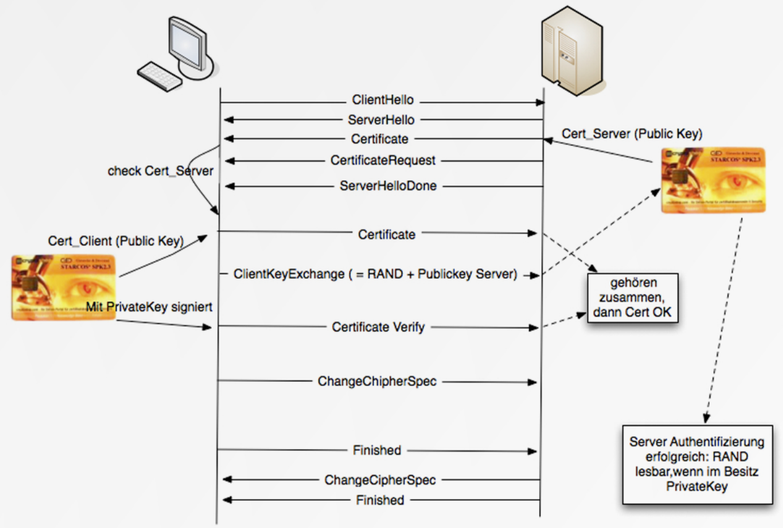
Aufbau einer Smart Card

Der Kartenkörper besteht in der Regel aus PVC (Polyvinylchlorid) und hat die Abmessung gängiger Scheckkarten (Format: 85,6 x 54 mm).

Zu den grundlegenden Hardwarekomponenten einer Smartcard gehören CPU, Speicher und eine Schnittstelle für die Kommunikation nach außen. Neben der eingesetzten CPU für die zentrale Logik der Karte können weitere Funktionen in zusätzlichen Hardwarechips stecken.

So ist es möglich kryptographische Coprozessoren oder Zufallszahlengeneratoren mit in die Karte zu integrieren. Dabei werden alle Komponenten innerhalb des Kunststoffs eingebettet. Nur die Kontakte sind von außen sichtbar. Über diese Kontakte wird die Smartcard mit der Betriebsspannung und dem Takt versorgt, sowie die eigentliche Kommunikation darüber abgewickelt.

Ablauf beidseitige Authentifizierung



Motivation

Ziel dieser Implementierung war eine starke beidseitige Client/Server-Authentifizierung umzusetzen.

Die Verschlüsselung, Integrität und Authentifizierung der Verbindung übernimmt das SSL-Protokoll. Um eine hohe Sicherheit zu gewährleisten ist sowohl das Client- als auch das Serverzertifikat jeweils auf einer Smartcard gespeichert.

Auf der Serverseite kommt der weit verbreitete Open Source Webserver Apache mit dem Modul mod_nss zum Einsatz

OpenSC Software Stack

Anwendung Firefox, Thunderbird, Apache, OpenSSH,...
OpenSC
OpenCT
Treiber
Hardware

Beschreiben einer Smart Card

1. Karte initialisieren
2. Benutzer-PIN und PUK erstellen
3. Erstellen der Schlüssel auf Karte
4. Erzeugen eines Zertifikats durch die Certificate Authority
5. Speichern des Zertifikats auf der Karte
6. Evtl. finalisieren der Karte

Kontakt
HdM Stuttgart - Medieninformatik
Timo Lenz, tl018@hdm-stuttgart.de
Christoph Baumann, cb057@hdm-stuttgart.de