eToken unter Linux

Frank Hofmann

Berlin

16. April 2009

Inhalt

Begriffsklärung

- Abkürzung für **e**lectronic **T**oken
- Smartcard mit Cryptoprozessor
- Kommunikation über die USB-Schnittstelle

Aladdin
SECURING THE GLOBAL VILLAGE

- Hersteller: Aladdin (Israel)
  deutsche Niederlassung: München

Sinn und Zweck

- zuverlässige Benutzerauthentisierung
- Zugangssicherung für sensible Bereiche
- Schutz von Daten und Privatspäre

- Risiken bei Benutzung von Passwörtern:
  - Verlust durch Diebstahl
  - „Vergessen“
  - Erraten und Knacken
  - geringe Überschaubarkeit der Zugangsdaten

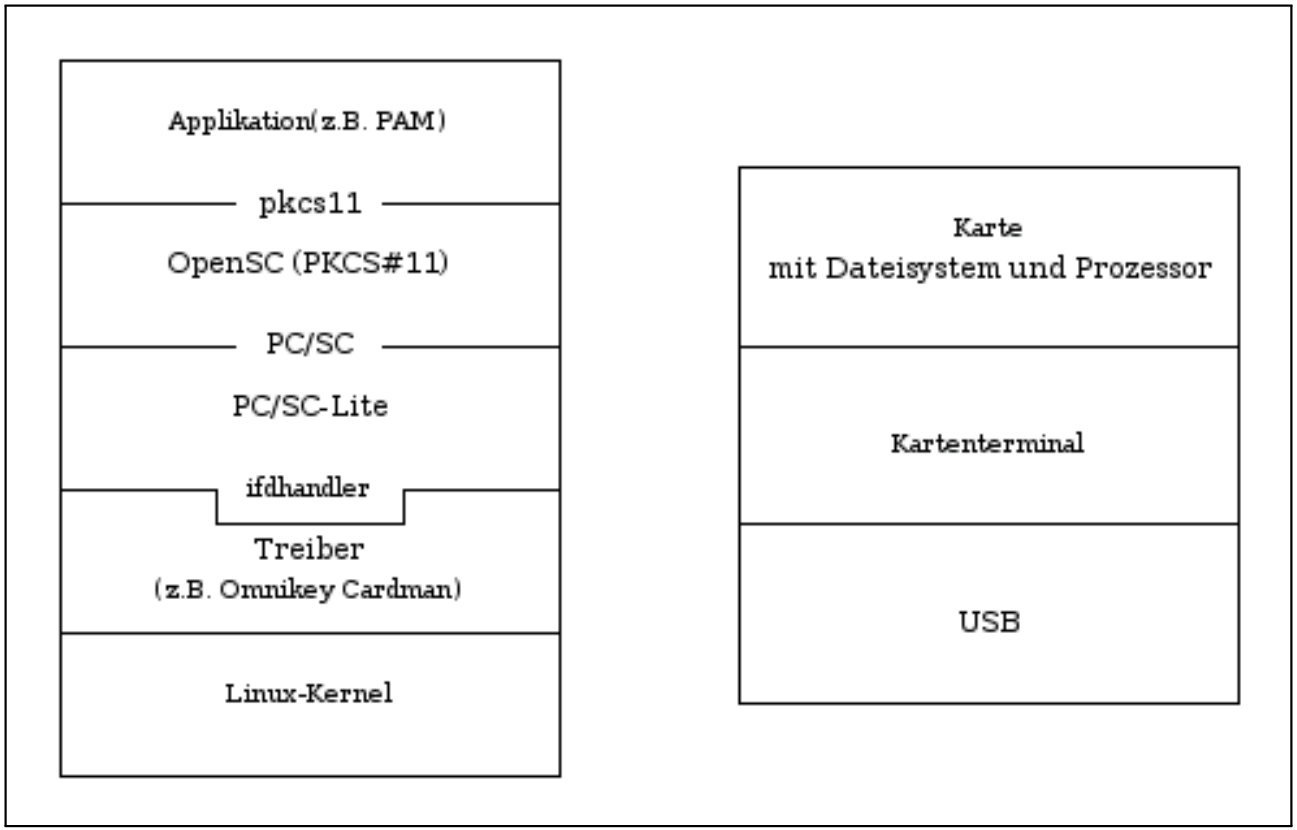
eToken-Varianten

- Unterstützte Betriebssysteme: W2K/XP/2003/Vista, Linux
- interner Speicher: 32K, 64K, 72K
- Sicherheitsverfahren: RSA 1024-bit / 2048-bit, DES, 3DES, SHA1
- APIs und Standards: PKCS#11 v2.01, Microsoft CAPI, PC/SC, X.509 v3-Zertifikatspeicherung, SSL v3, IPSec/IKE
- Lagertemperatur: -40 bis 85 Grad C
- Datenverbleib im Speicher: bis zu 10 Jahre

eToken-Varianten und Preise

- eToken Pro: ab ca. EUR 30.00 (Einzelpreis)

Softwarestack (Linux) (1)



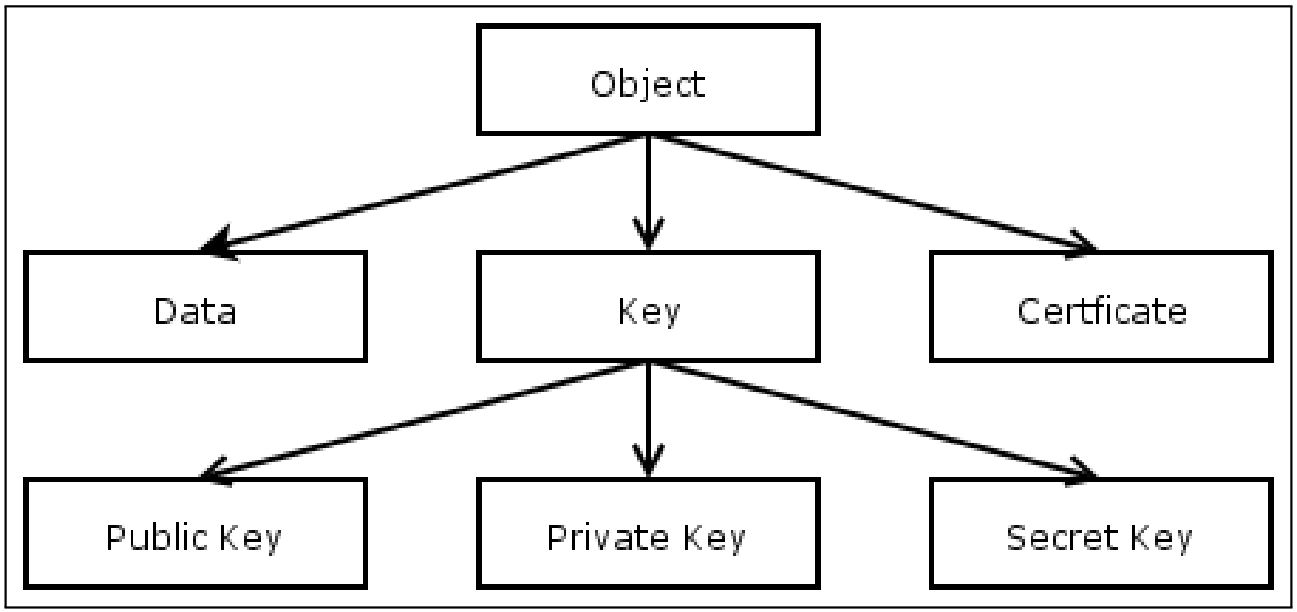
Softwarestack (Linux) (2)

- Pluggable Authentication Modules (PAM)
  Softwarebibliothek, allgemeine Programmierschnittstelle (API) für Authentisierungsdienste
- Public Key Cryptography Standards (PKCS#11/Cryptoki)
  Programmierschnittstelle für Security Tokens und Smartcards
- OpenSC
  Sammlung von Bibliotheken zur Kommunikation mit Smartcards
- PC/SC
  Abstraktionsschicht für den Cardreader
- ifd-Handler
  Handler für die Schnittstelle

Der PKCS#11-Standard (1)

- eToken aus Sicht des PKCS#11:
  Gerät, das Objekte speichert und darauf kryptografische Funktionen ausführen kann
- Objekte (Daten, Zertifikate, Schlüssel)
  Verfügbarkeit: öffentlich oder privat
- 2 Benutzer:
  - Eigentümer (Zugriff auf private Objekte)
  - Security Officer (SO) (Zugriff auf öffentliche Objekte)
- Applikationen: Kommunikation über Sessions
  Lesen und Schreiben von Objekten

Der PKCS#11-Standard (2)



OpenSC (1)

- Smartcard-Framework für Linux, Mac und Windows
- Untstützt viele digitalen Personalausweise
- Unterprojekte
  - OpenCT: Treiber für Smartcardreader
  - pam_p11: einfaches Modul zur Benutzeranmeldung
  - pam_pkcs11: ausgereifter und mehr Features
  - Java-Bindings
  - PKCS#11-Bibliotheken

OpenSC - Tools (2)

- Angeschlossene Smartcards/eToken anzeigen
  `opensc-tool -l -vv`
- Informationen über das eToken-OS anzeigen
  `cardos-info -r 0`
- eToken initialisieren
  `pkcs11-tool --init-token`
- Speicherinhalt anzeigen
  `openct-tool -r0 mf`
- Inhalt des eToken erforschen
  `opensc-explorer`
- Alle Files des eToken anzeigen
  `opensc-tool -f -vv`

Anwendungen (1)

http://www.etokenonlinux.org/et/Applications_for_eToken

- Mozilla Firefox, Thunderbird
- openssh
- rdesktop
- truecrypt
- OpenVPN
- StrongSwan

Anwendungen (2)

Alon Barlev
`http://alon.barlev.googlepages.com/open-source`

- OpenVPN, OpenSSH
- Qt Cryptographic Architecture (QCA)
- GnuPG
- eCryptfs Linux filesystem
- GnuTLS
- MySQL
- Linux Disk Encryption Integration (suspend, Loop-AES, fbsplash, Smartcards)

APIs und Beschreibungen der einzelnen Tools

- Tools
  - OpenSC-Tools
    `/usr/share/doc/opensc/tools.html`
- Libraries und APIs
  - libopensc2-dev (C/C++)
    `/usr/share/doc/libopensc2-dev/api.html`
  - PyKCS11 (Python)
    `http://pypi.python.org/simple/pykcs11/`

eToken – Vor- und Nachteile

Vorteile

- ein USB-Device für alle Zugangsdaten
- starke Authentisierung
- kein Backup möglich
- Verwendung verbreiteter Schnittstellen
- Einfachheit, Portabilität
- Robustheit
- Reduktion des Verwaltungsaufwands

Nachteile

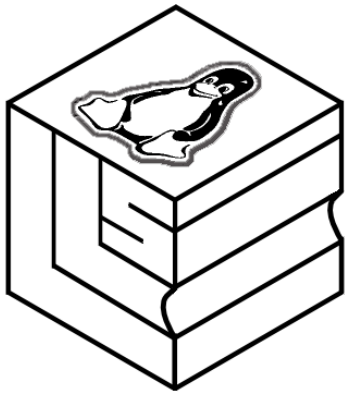
- ein USB-Device für alle Zugangsdaten
- begrenzte Anzahl Speicherplatz
- Unterstützung für ausgewählte Software
- überschaubare Dokumentation
- kein Backup möglich

Links

- OpenSC
  `http://www.opensc.org`
- etokenonlinux
  `http://www.etokenonlinux.org`
- Humboldt-Universität Berlin
  `http://sarwiki.informatik.hu-berlin.de/Smartcard_Based_Authentication`
- PyKCS11
  `http://www.bit4id.org/trac/pykcs11`
- Movement for the Use of Smartcards in a Linux Envinronment (MUSCLE)
  `http://www.linuxnet.com/`

Vielen Dank!

Danke für Eure Aufmerksamkeit :-)



Kontakt:
Dipl.-Inf. Frank Hofmann
Hofmann EDV – Linux, Layout und Satz
c/o büro 2.0
Weigandufer 45 – 12059 Berlin
Email <frank.hofmann@efho.de>
web www.efho.de