Using eTokens with Linux

Frank Hofmann

Berlin

3. Oktober 2009

Contents

Terms

- Abbreviation for **e**lectronic **T**oken
- Smartcard with cryptographic processor
- Communication via USB interface

Aladdin
SECURING THE GLOBAL VILLAGE

- Supplier: Aladdin (Israel)
  German office: München

Intention and Purpose

- Reliable user authentication
- Access mechanism for sensitive areas
- Protection of data and privacy

- Risks using passwords:
  - loss by theft
  - „forgotten“
  - guess and crack
  - low manageability of access data

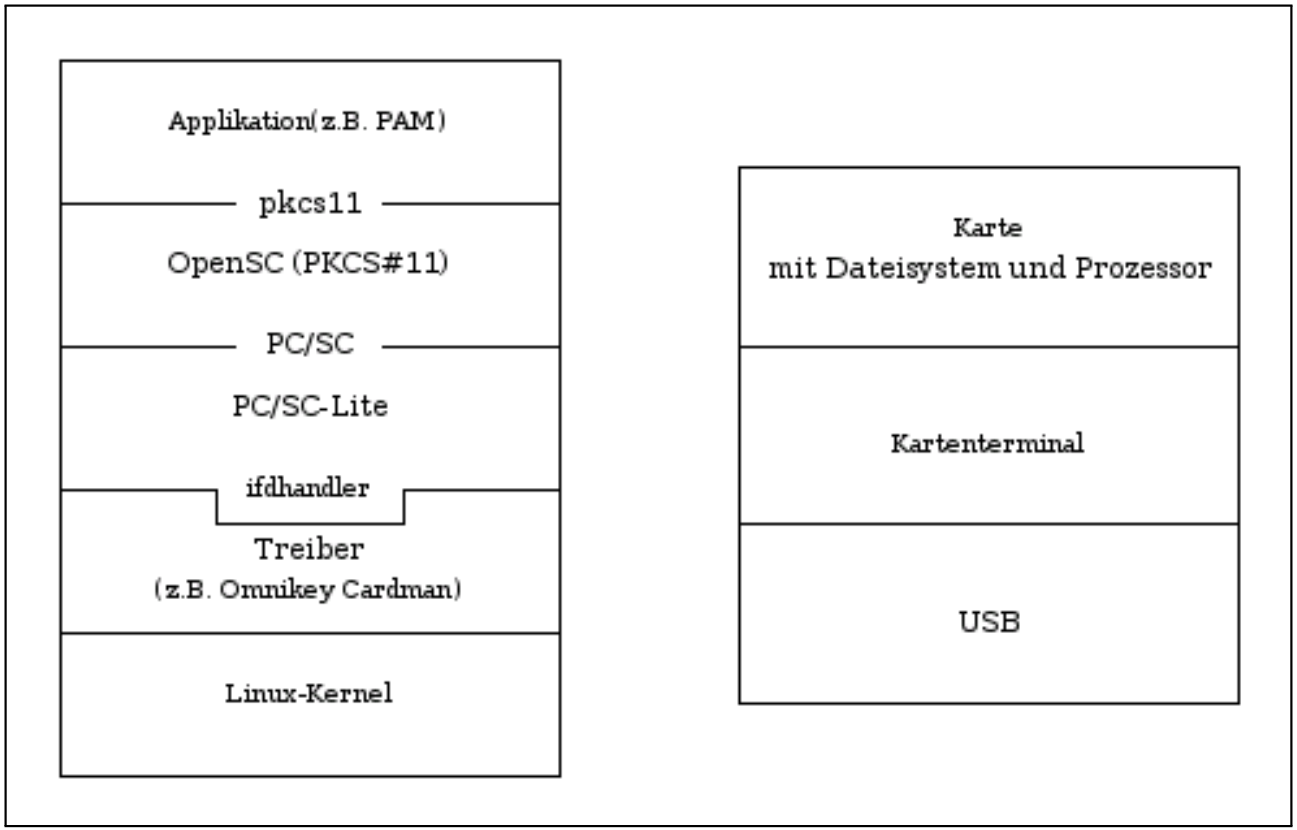
Variants of eToken

- Supported operating systems: W2K/XP/2003/Vista, Linux
- Internal memory: 32K, 64K, 72K
- Security mechanisms: RSA 1024-bit / 2048-bit, DES, 3DES, SHA1
- APIs and standards: PKCS#11 v2.01, Microsoft CAPI, PC/SC, X.509 v3 certificates, SSL v3, IPSec/IKE
- Storage temperature: -40 to +85 Grad C
- Data storage warranty: 10 years

Variants and Pricing

- eToken Pro: ca. EUR 30.00 (single price)

Software stack (Linux) (1)



Software stack (Linux) (2)

- Pluggable Authentication Modules (PAM)
  software library, general API for authentication services
- Public Key Cryptography Standards (PKCS#11/Cryptoki)
  programming interface for security tokens and smartcards
- OpenSC
  collection of libraries for the communication with smartcards
- PC/SC
  card reader abstraction layer
- ifd handler
  interface handler

The PKCS#11 Standardization

- PKCS#11 view for an eToken:
  a device that saves objects that allow cryptographic functions with
- Objects (data, certificates, keys)
  availability: public or private
- 2 users:
  - Owner (access for private objects only)
  - Security Officer (SO) (access for public objects only)
- Applications: session-based communications
  reading and writing of objects

OpenSC (1)

- Smartcard framework for Linux, Mac and Windows
- Supports digital identity cards
- Collection of sub-projects:
  - OpenCT: driver for smartcard reader
  - pam_p11: simple module for user login
  - pam_pkcs11: sophisticated module with more features
  - Java bindings
  - PKCS#11 libraries

OpenSC - Tools (2)

- Display connected smartcards/eToken
  `opensc-tool -l -vv`
- Display information about the eToken OS
  `cardos-info -r 0`
- Initialize an eToken
  `pkcs11-tool --init-token`
- Display contents of the memory
  `openct-tool -r0 mf`
- Explore the contents of the eToken
  `opensc-explorer`
- Display all files saved on the eToken
  `opensc-tool -f -vv`

Applications (1)

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

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

Applications (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 and Descriptions for these Tools

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

eToken – advantages and disadvantages

Advantages

- one single USB device containing all access data
- strong authentication
- no backup possible
- usage of common interfaces
- simplicity, portability
- robustness
- reduction of administrative effort

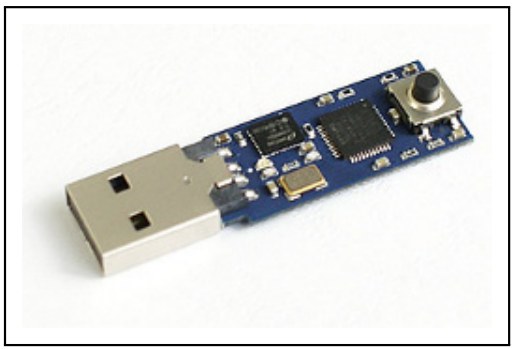
Disadvantages

- one single USB device containing all access data
- limited memory
- support for selected software, only
- limited documentation
- no backup possible

eToken – Alternative Tools (1)

openkubus

`http://code.google.com/p/openkubus/`



- Simple framework for secure authentication using automatically generated one-time-pads
- Hardware layout available for free
- Can be easily integrated into existing programms
  libraries for C, Perl and PHP
  a server and a PAM module

eToken – Alternative Tools (2)

GPFCryptoStick by the German Privacy Foundation

`https://www.privacyfoundation.de/wiki/GPFCryptoStick`

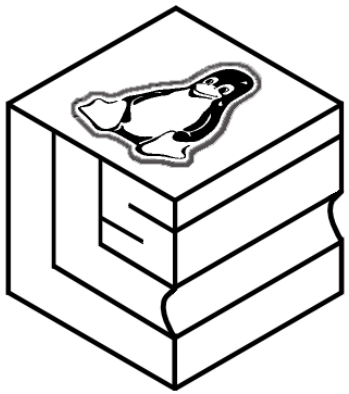
- USB stick with OpenPGP smartcard
- 3 independent 1024 Bit RSA keys (sign, crypt, authenticate)
- Creation of keys on the card and/or import of existing keys, whereas the secret key never leaves the on-board chip
- Compatible for Linux and Windows

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/`

Many thanks!

Thanks for your attention :-)



Contact:
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

YES, WE ARE OPEN!
büro2.0
Open Source Bürogemeinschaft & Expertennetzwerk

web www.buero20.org