Debian and smart cards

Ludovic Rousseau
Debian Miniconf Paris, Oct. 2010
Agenda

• Who am I?
• What is a smart card
• Smart cards packages in Debian
• Why use a smart card
• What to buy?
• Online information
• Conclusion
Who am I?

- Debian user since 1998
- Debian Developer since 2001

Packages I maintain:
  - smart card
    - pcsc-lite ccid pcsc-perl pcsc-tools asedriveiiiie coolkey ifd-gempc libmusclecard muscleframework muscletools pam-pkcs11 pykcs11 pyscard xcardii
  - Palm PDA
    - jpilot jpilot-backup pilot-link plucker
  - Misc
    - bins colormake jhead
What is a smart card?

- Piece of plastic + micro controller
- 3 formats (ISO 7816-1):
  - ID-1 (full size)
  - ID-000 (SIM plugin size)
  - Micro-SIM
- Micro controller (ISO 7816-2)
Communication protocol: ISO 7816-3

- Half duplex communication
- External clock: ~4 MHz
- 2 protocols: T=0, T=1
- ATR: Answer To Reset
- PTS: Protocol Type Selection

- Communication is taken care by the software layers
  - IFD handler (driver)
  - PC/SC layer (middleware)
Commands: ISO 7816-4

- APDU: APplication Data Unit
  - Header: CLAss, INStruction, Parameter 1, Parameter 2
  - Data
- Example: VERIFY
  - 80 20 00 00 04 31 32 33 34

- Lots of commands defined
  - Standards are not complete
  - Cards manufacturers diverge from standards
Private/proprietary specifications

- French banking cards: Carte bancaire B0'
- French health cards: Carte Vitale
- Pay TV cards

It is hard to correctly use such cards... but not always impossible
http://parodie.com/monetique/explorer.htm
Publicly documented specifications

- EMV bank cards
- GSM/3G cards
  - GSM 11.11/ETSI 102 221
- Some National ID/eID cards
  - IAS/ECC: Identification-Authentication-Signature
    European-Citizen-Card
- Some PKI cards
  - SetCOS, ACOS5
- Biometric Passport (ICAO)
- OpenPGP card
  - [http://www.g10code.de/p-card.html](http://www.g10code.de/p-card.html)
Programmable smart cards

- JavaCard
  - a free software MUSCLE applet is available
- .NET
  - not yet tried
- BasicCard
  - example: OpenPGP V1 and V2 cards
- Multos
- GlobalPlatform
Debian packages for smart cards

- http://people.debian.org/~rousseau/smartcard.html
- 12 reader drivers
  - libacr38u libacr38ucontrol0 libacr38ucontrol-dev libbasedrive-serial libbasedrive-usb libccid libchipcardc2 libgcr410 libgempc410 libgempc430 libtowitzitoko2 libtowitzitoko-dev
- 42 middlewares/libraries
  - coolkey libbeid2 libbeid2-dbg libbeid2-dev libbeidlibopensc2 libbeidlibopensc2-dbg libbeidlibopensc2-dev libcflexplugin libchipcard-ctapi0 libchipcard-data libchipcard-dev libchipcard-libgwenhywfar47-plugins libchipcard-tools libckyapplet1 libckyapplet1-dev libengine-pkcs11-openssl libmcardplugin libmusclecard1 libmusclecard-dev libmusclepkcs11 libmusclepkcs11-dev libopenetc1 libopenetc1-dbg libopenetc1-dev libopenetc2 libopenetc2-dbg libopenetc2-dev libpam-musclecard libpam-p11 libpam-pkcs11 libpam-poldi libpcscada0.6 libpcscada1-dev libpcscslite1 libpcscslite-dev libpcscl-lite perl mozilla-opensc openct pam-pkcs11-dbg pcscada-dbg pcscd python-pyscard
- 16 applications
  - beidgui beid-tools esteidutils gnokii gnupg gnupg2 hostapd libchipcard-tools muscletools opensc pcsc-tools rdesktop virtualbox-ose wine wpasupplicant xcardii
CCID: Circuit(s) Cards Interface Devices

- USB specification available on http://www.usb.org/
- Define bInterfaceClass = 11 (0x0b)
- Goal: replace all the proprietary protocols by only one

- libccid: free software CCID driver
  - http://pcsclite.alioth.debian.org/ccid.html
  - 180 readers supported (or partly supported)
PC/SC: Personal Computer Smart Card

- Specification from PC/SC workgroup
  - http://www.pcscworkgroup.com/
- Implemented by Microsoft in Windows

- pcsc-lite: free software implementation of the API
  - http://pcsclite.alioth.debian.org/
  - should be the only smart card API used on Unix
    - Apple fork (Roseta)
    - SUN fork (SunRay)
PKCS#11: Cryptographic Token Interface Standard

• RSA labs defined API for PKI tokens
  ◦ smart cards
  ◦ software tokens (Firefox includes one)
  ◦ PCI cards (IBM 4758)

• OpenSC: free software implementation of the API
  ◦ using smart cards
  ◦ https://www.opensc-project.org/opensc
pyscard: Python PC/SC wrapper

- http://pyscard.sourceforge.net/
- Direct PC/SC API
  - fine control of everything
  - I use it to write pcsc-lite Unitary Tests
- Higher level API
  - less code to write
PyKCS11: Python PKCS#11 wrapper

- http://www.bit4id.org/trac/pykcs11
- Low level API
- High level API

- Sample code soon available on my blog
Big picture

Many other software are available (but not displayed)
What can a smart card be used for?

• In a computing system (PKI) using PKCS#11
  ◦ Local user authentication (PAM)
  ◦ Web SSL client authentication
  ◦ Mail signature
  ◦ Mail deciphering
  ◦ SSH client authentication

• Two factor authentication
  ◦ what I own: smart card
  ◦ what I know: PIN code
Electronic ID cards

• Some european citizen already have an eID card
  ◦ Estonia  http://www.id.ee/?lang=en

• Most european citizens will receive an eID card (soon)
  ◦ Spain  http://www.dnielectronico.es/
  ◦ Portuguese
  ◦ France  http://www.ants.interieur.gouv.fr/ias/-ias-.html
  ◦ Belgium  http://eid.belgium.be/
  ◦ Germany
    ▪ Nov 2010
  ◦ Luxembourg
    ▪ Q1 2011
What to buy?

- Smart card reader
  - CCID reader supported by libcccid
  - contact, contactless or both?

- Smart card
  - PKI smart card supported by OpenSC
  - OpenPGP card
  - JavaCard and install the Muscle applet
Online information about smart cards and Free Software

- Wikipedia
- Muscle mailing list
  - http://musclecard.com/list.html
- OpenSC mailing lists
  - https://www.opensc-project.org/opensc/wiki/MailingLists
- My blog
  - http://ludovicrousseau.blogspot.com/
For more information (in french)
Conclusion

• Many smart card programs are in Debian
  ◦ just one "apt-get install" away

• Free Software smart card?
  ◦ all cards contain a proprietary "firmware"
Thanks

• Wikipedia for the images and information
• You for your participation

Questions?