The eID

Wouter Verhelst

Debian GNU/Linux

Journées du Libre, 8 may 2009

The card: hardware

- Javasomething card

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15
- identity data/picture stored in file on card, specs public

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15
- identity data/picture stored in file on card, specs public
- weirdness:

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15
- identity data/picture stored in file on card, specs public
- weirdness:
  - two keys: signature and authentication

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15
- identity data/picture stored in file on card, specs public
- weirdness:
  - two keys: signature and authentication
  - Cannot log in to signature key

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15
- identity data/picture stored in file on card, specs public
- weirdness:
  - two keys: signature and authentication
  - Cannot log in to signature key
  - one PIN

The card: hardware

- Javasomething card
- implements subset of PKCS#11, PKCS#15
- identity data/picture stored in file on card, specs public
- weirdness:
  - two keys: signature and authentication
  - Cannot log in to signature key
  - one PIN

Privacy issues

- National identification number embedded in certificates

Privacy issues

- National identification number embedded in certificates
- Copying data vs viewing it

Privacy issues

- National identification number embedded in certificates
- Copying data vs viewing it
- ...

Key secrecy

- Traditional smartcard: bought empty, keys stored or generated by user

Key secrecy

- Traditional smartcard: bought empty, keys stored or generated by user
- eID card: keys generated by manufacturer/municipal office

Key secrecy

- Traditional smartcard: bought empty, keys stored or generated by user
- eID card: keys generated by manufacturer/municipal office
- legal issues: knowledge of PIN, ownership of card = legal signature

Software: overview

- libbeidlibopensc.so.2: central library from OpenSC, modified to show login dialog when needed using libqt

Software: overview

- libbeidlibopensc.so.2: central library from OpenSC, modified to show login dialog when needed using libqt
- libbeid.so.2: high-level library to retrieve identity information

Software: overview

- libbeidlibopensc.so.2: central library from OpenSC, modified to show login dialog when needed using libqt
- libbeid.so.2: high-level library to retrieve identity information
- beidgui: graphical application to read info on smartcard/change pin

Software: overview

- libbeidlibopensc.so.2: central library from OpenSC, modified to show login dialog when needed using libqt
- libbeid.so.2: high-level library to retrieve identity information
- beidgui: graphical application to read info on smartcard/change pin
- Mozilla plugin: sign/authenticate under Mozilla Firefox, Mozilla Thunderbird, OpenOffice.org, ...

Software: overview

- libbeidlibopensc.so.2: central library from OpenSC, modified to show login dialog when needed using libqt
- libbeid.so.2: high-level library to retrieve identity information
- beidgui: graphical application to read info on smartcard/change pin
- Mozilla plugin: sign/authenticate under Mozilla Firefox, Mozilla Thunderbird, OpenOffice.org, ...
- OpenSC: **Open S**mart **C**ard framework, to access/use smartcards.

Software: overview

- libbeidlibopensc.so.2: central library from OpenSC, modified to show login dialog when needed using libqt
- libbeid.so.2: high-level library to retrieve identity information
- beidgui: graphical application to read info on smartcard/change pin
- Mozilla plugin: sign/authenticate under Mozilla Firefox, Mozilla Thunderbird, OpenOffice.org, ...
- OpenSC: **Open S**mart **C**ard framework, to access/use smartcards.
- (MS Office plugin/other Windows-specific software)

Debian packages

- beidgui

Debian packages

- beidgui
- libbeidlibopensc2 (-dbg, -dev)

Debian packages

- beidgui
- libbeidlibopensc2 (-dbg, -dev)
- libbeid2 (-dbg, -dev)

Debian packages

- beidgui
- libbeidlibopensc2 (-dbg, -dev)
- libbeid2 (-dbg, -dev)
- beid-tools

Debian packages

- beidgui
- libbeidlibopensc2 (-dbg, -dev)
- libbeid2 (-dbg, -dev)
- beid-tools
- opensc

Debian packages

- beidgui
- libbeidlibopensc2 (-dbg, -dev)
- libbeid2 (-dbg, -dev)
- beid-tools
- opensc
- libopensc2 (-dev, -dbg)

Debian packages

- beidgui
- libbeidlibopensc2 (-dbg, -dev)
- libbeid2 (-dbg, -dev)
- beid-tools
- opensc
- libopensc2 (-dev, -dbg)
- libacr38u

beidgui

- Cross-platform application

beidgui

- Cross-platform application
- Uses libbeidlibopensc/libbeid

beidgui

- Cross-platform application
- Uses libbeidlibopensc/libbeid
- (demo)

Mozilla plugin

- to load in firefox: beid-pkcs11-register.html, or manually

Mozilla plugin

- to load in firefox: beid-pkcs11-register.html, or manually
- to load in thunderbird: load manually

Mozilla plugin

- to load in firefox: beid-pkcs11-register.html, or manually
- to load in thunderbird: load manually
- openoffice: load in firefox, then point openoffice to mozilla configuration directory.

Reading certificate info

- pkcs15-tool -c

Reading certificate info

- pkcs15-tool -c
- pkcs11-tool -r <nr> | openssl x509 -noout -text

OpenSC/OpenSSH: logging in to a remote server

Requirements: OpenSSH with OpenSC compiled in, cardreader

OpenSC/OpenSSH: logging in to a remote server

Requirements: OpenSSH with OpenSC compiled in, cardreader

- `ssh-keygen -D 0 > id_eID.pub`
- copy id_eID.pub to remote server, add to `.ssh/authorized_keys`
- log in to card; e.g., `beid-pkcs11-tool -l -t`
- `ssh -I 0 <server>`