Using the Belgian eID card on CentOS Linux

Fabian Arrotin
fabian.arrotin@arrfab.net
Agenda

- Introduction
- Belgian eID presentation
- Which software is needed to interact with the eID?
- Installation of programs with yum
- Viewing information on the eID
- Using Firefox and Thunderbird with the eID
- Using the eid reverse proxy on Linux
Belgian eID presentation

- Issued to every Belgian citizen starting from Sept 2005
- Every citizen will have eID for end 2009
- Only for people who are 12+ old
- Kids eIDs exist but don't contain certificates
- Based on JavaCard technology
- Private keys can not leave the eID!
- Only manageable by the Belgian government
Estimated number of eID

Graphs kindly copied from http://godot.be/eidgraphs
EID card overview
Certificates sitting on the eID

- 0 – 6 years: Kids card: no certificates
- 6 – 12 years: Kids card: authentication certificate
- 12 – 18 years: eID card: authentication certificate
- 18 - +: eID card:
  - Authentication certificate
  - Digital signature certificate

Certificates can be deactivated on citizen request
Which software is needed?

- pkg-config 0.15.0 (or greater)
- pcsc-lite 1.2.9 (or greater, not included in CentOS base)
- Qt 3.3.3 (or greater)
- Python 1.5.2 (or greater)
- openssl 0.9.7 (or greater)
- WxGTK 2.4 (or greater, not included in CentOS base)
- Specific card reader driver for pcsc-lite ! (or opensc)
Installing automagically with yum

- Configure yum to use the RPMForge repository (http://wiki.centos.org/Repositories/RPMForge)
- `yum install eid-belgium pcsc-lite`
- Don't forget your specific card reader driver!
- Example: `yum install pcsc-lite-acr38u`
- Remark: at this time, only the pcsc-lite driver for ACR38U (the most used card reader) is packaged and available in rpmforge
 Commands available

- beid-tool -l (to list the reader)
- beid-pkcs11-tool -t -l --module /usr/lib/libbeidpkcs11.so (to test connectivity with the eID)
- beidgui (GUI)
1. Web server sends challenge to the browser
2. Citizen confirms authentication procedure by entering the pin
3. Browser sends hashed challenge to the eID to sign in
4. Browser gets signature and certificate from the eID
5. Web server receives signature and certificate
Using Firefox and Thunderbird with the eID

- You first need to load the security device module:
- Launch firefox (same for thunderbird) / preferences / advanced / security / security devices

Select 'Load' and point to /usr/lib/libbeidpkcs11.so.2
Using the eID reverse proxy

- Multi-platform solution for authenticating citizens with their eID card on a Web Server/application server.
- Contains modified Apache package (updated version of “mod_ssl” to support the OCSP protocol).
- No rpm package (yet) ...
Useful resources

- [http://www.eid.belgium.be](http://www.eid.belgium.be) (official website)
- [http://homes.esat.kuleuven.be/~decockd/wiki/bin/view.cgi](http://homes.esat.kuleuven.be/~decockd/wiki/bin/view.cgi) (Danny De Cock's website, thanks for the graphs)
These slides will be available on
http://wiki.centos.org/Events/Fosdem2007/
in pdf format.