

# *Using the Belgian eID card on CentOS Linux*

Fabian Arrotin  
fabian.arrotin@arrfab.net

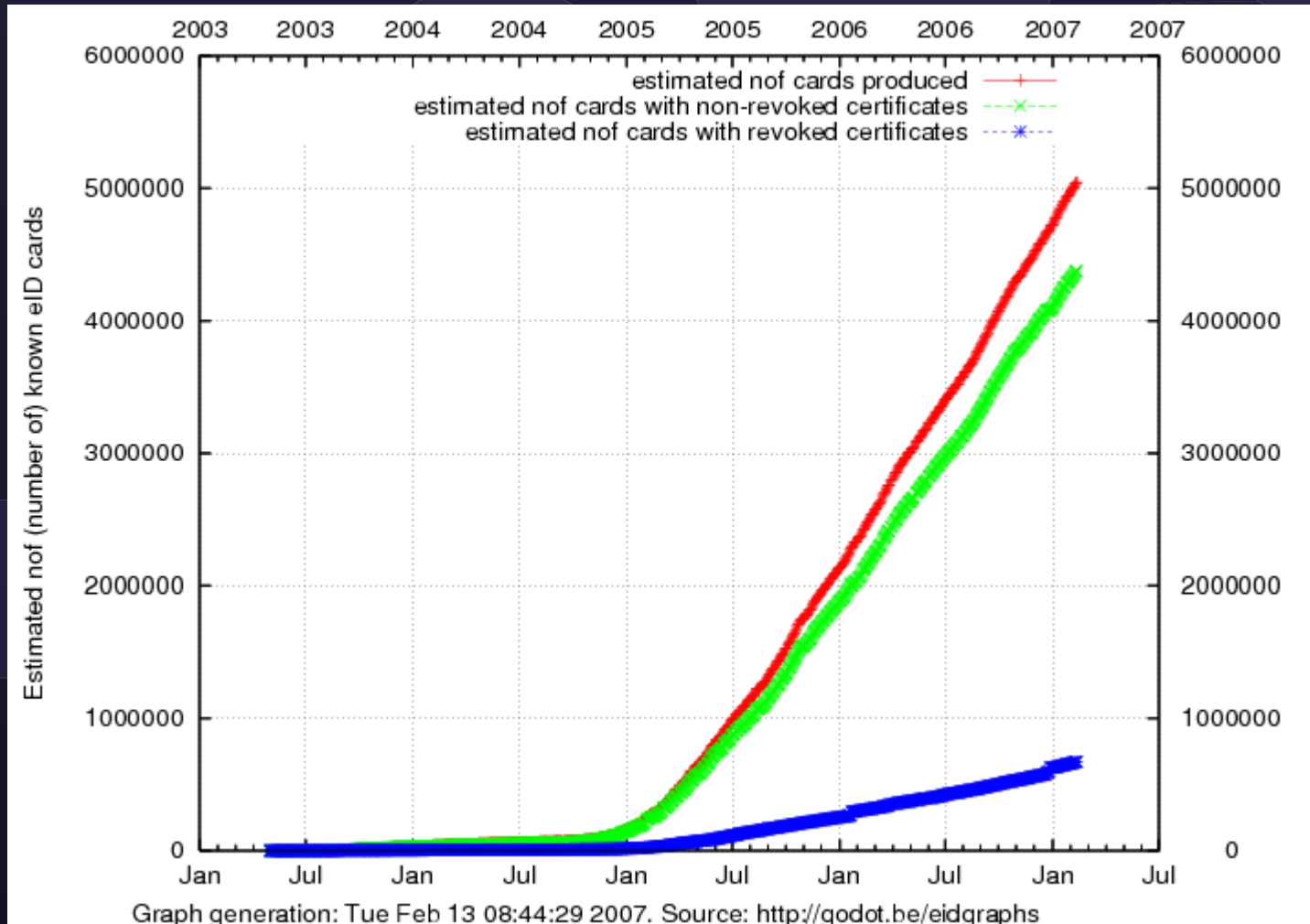
# Agenda

- 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
- Middleware source code available for the citizen (available on [http://www.belgium.be/zip/eid\\_datacapture\\_fr.html](http://www.belgium.be/zip/eid_datacapture_fr.html) or [http://www.belgium.be/zip/eid\\_datacapture\\_nl.html](http://www.belgium.be/zip/eid_datacapture_nl.html) )

# 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*

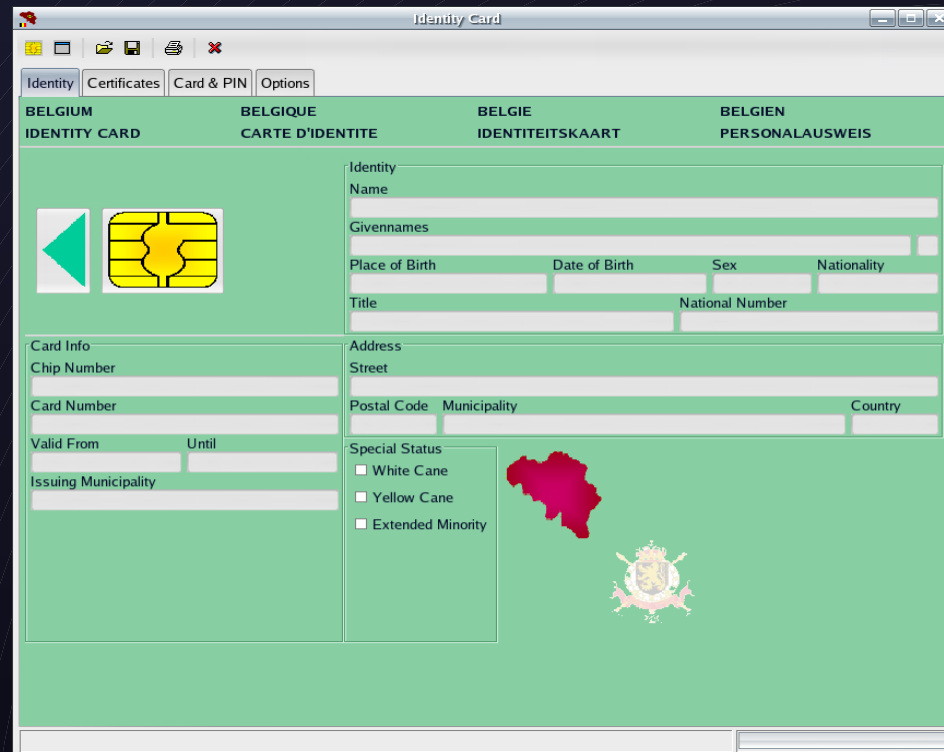
- Configure yum to use the RPMForge repository ( <http://wiki.centos.org/Repositories/RPMForge> )
- yum install eid-belgium pcsc-lite
- Don't forget your specific card reader driver !
- example : yum install pcsc-lite-acr38u
- Remark : at this time, only the pcsc-lite driver for ACR38U (the most used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





# Commands available

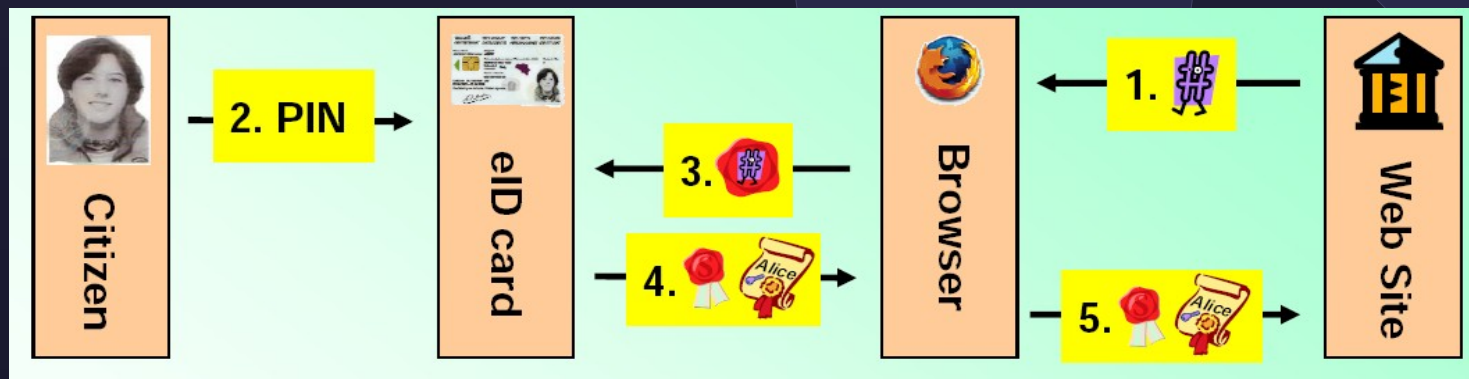
- `beid-tool -l` (to list the reader)
- `beid-pkcs11-tool -t -l --module /usr/lib/libbeidpkcs11.so` (to test connectivity with the eID)
- `beidgui` ( GUI )



The screenshot shows the 'Identity Card' GUI application window. The window title is 'Identity Card'. It has a menu bar with 'Identity', 'Certificates', 'Card & PIN', and 'Options'. The main content area is divided into several sections:

- Language Selection:** Four buttons for 'BELGIUM IDENTITY CARD', 'BELGIQUE CARTE D'IDENTITE', 'BELGIE IDENTITEITSKAART', and 'BELGIEN PERSONALAUSWEIS'.
- Identity Section:** Includes a back arrow, a yellow chip icon, and fields for Name, Givennames, Place of Birth, Date of Birth, Sex, Nationality, Title, and National Number.
- Card Info Section:** Includes fields for Chip Number, Card Number, Valid From, Until, and Issuing Municipality.
- Address Section:** Includes fields for Street, Postal Code, Municipality, and Country.
- Special Status Section:** Includes radio buttons for 'White Cane', 'Yellow Cane', and 'Extended Minority'.
- Map and Logo:** A red map of Belgium and the national coat of arms are displayed.

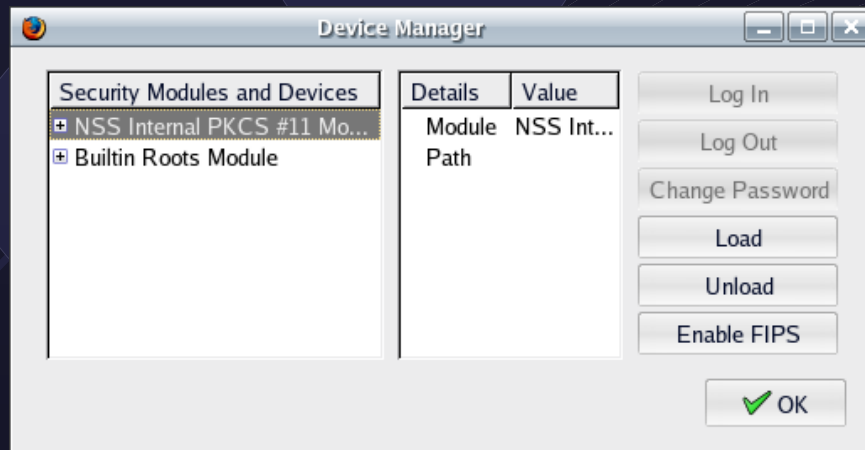
# Browser session



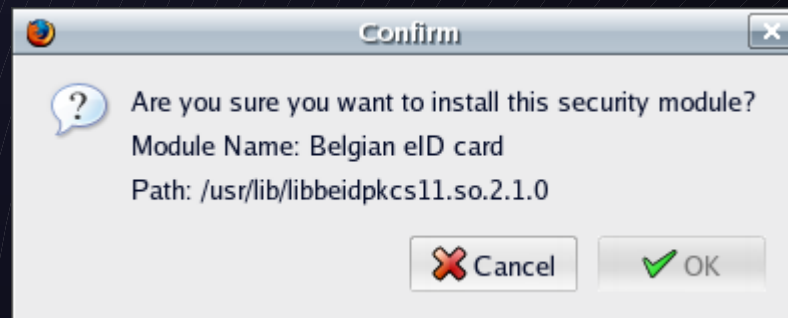
1. Web server sends challenge to the browser
2. Citizen confirms authentication procedure by entering the pin
3. Browser sends hashed challenge to the eID to sign in
4. Browser gets signature and certificate from the eID
5. Web server receives signature and certificate

# 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

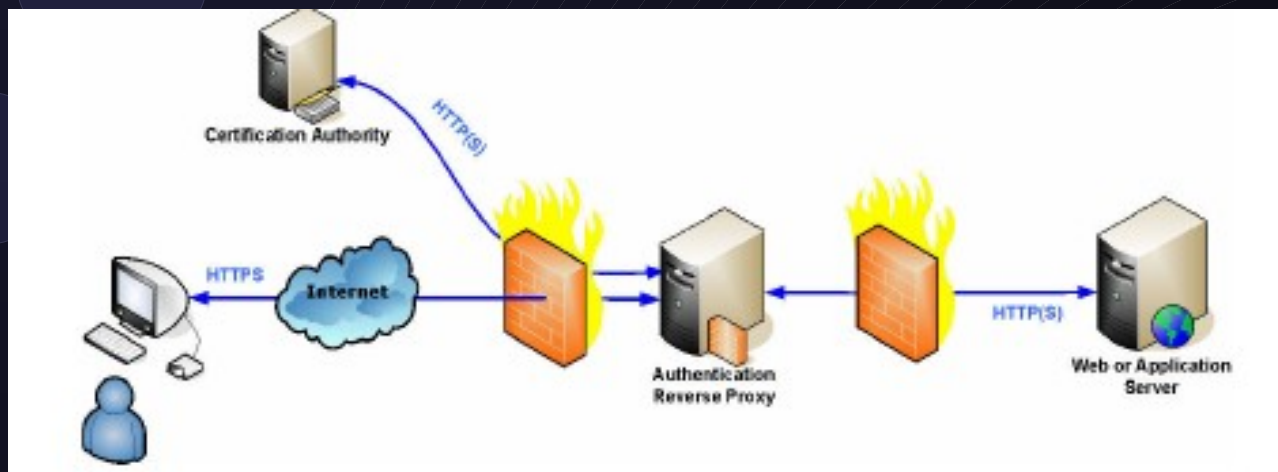


- Select 'Load' and point to `/usr/lib/libbeidpkcs11.so.2`



# Using the eID reverse proxy

- multi-platform solution for authenticating citizens with their eID card on a Web Server/application server
- Publicly available on [http://www.belgium.be/zip/eid\\_authentication\\_proxy\\_fr.html](http://www.belgium.be/zip/eid_authentication_proxy_fr.html) or [http://www.belgium.be/zip/eid\\_authentication\\_proxy\\_nl.html](http://www.belgium.be/zip/eid_authentication_proxy_nl.html)
- Contains modified Apache package (updated version of “mod\_ssl” to support the OCSP protocol2)
- No rpm package (yet) ...



# *Useful resources*

- <http://www.eid.belgium.be> (official website)
- <http://homes.esat.kuleuven.be/~decockd/wiki/bin/view.cgi>  
(Danny De Cock's website, thanks for the graphs)
- <http://dag.wieers.com/rpm/packages/eid-belgium/>  
(Dag Wieers' website, rpm packager for RPMForge)



# *Questions ?*

These slides will be available on  
<http://wiki.centos.org/Events/Fosdem2007/>  
in pdf format.