FriBID

A free and open Swedish BankID client

Henrik Nordström

henrik@henriknordstrom.net

Open Source Wizard, Squid, Linux & Networking since 1995

What is BankID

- BankID is the leading electronic identification in Sweden
- Based on PKI infrastructure with a PKI
- No public specification
- Special proprietary client program required
- Soft file based certificates
- Hard smartcard certificates

Nexus Personal

- Official BankID client for Windows, MacOS and Ubuntu 8.04 32-bit
- No 64-bit linux support
- Large progra with a number of browser plugins with unknown functionality

FriBID

- Free & Open BankID client
- fribid.se
- Samuel Lidén Borell
- Smartcard support
- Protocol based reverse enginerring, looking at input/output of the plugin.

Current status

- Login & signing transactions
- Hard smartcard certificates
- Soft filebased certificates
- No import från Nexus Personal
- Can't yet create new soft certificates

Why no import

- Keys exported by Nexus Personal is encrypted
- Encryption key is based on USB media used for export (USB key serialnumber + entered password + secret algorithm)

Future

- Request new soft certificates
- Lobbying for open specifikationer for electronic identification in sweden
- Lobbying for open drivers to smartcard readers

Reverse engineering

- BankID plugin javascript
- Analysis of HTML + Javascript
- Custom test pages exploring the Javascript API
- Based on open message format specifications
- xmldsig (login & signing)
- PKCS#10 wrapped in PKCS#7 / CMS (certificate signing request)
- X509 (certificate format)

Thank you

www.fribid.se