

# HARDWARE CRYPTO DEVROOM

F O S D E M

0 5 . 0 2 . 2 0 1 1 B R U S S E L S

OPENSC

[WWW.OPENSC-PROJECT.ORG](http://WWW.OPENSC-PROJECT.ORG)

# MOTIVATION FOR THE DAY

☀ “What good are PKI smart cards if you cant use them?”

☀ Library integration (SSL/TLS, SSH)

libssh overview, libcurl as an example, CyaSSL intro

☀ Making PKCS#11 more usable and useful

Trust assertions - GnomeKeyring, unified access - GnuTLS

☀ Full use cycle: initialization, personalization, use

RA/CA: EJBCA, use in browsers beyond SSL - Fribid

☀ Other interesting talks about security

OATH: Dynalogin, rootkits: SystemTap

# SCHEDULE

- ✿ 13.15 Smart card jungle (Jean-Michel Pouré, [gooze.eu](http://gooze.eu))
- ✿ 13.45 SSH libraries; libssh (Aris Adamantiadis, libssh)
- ✿ 14.15 libcurl: supporting 7 SSL libraries and 1 SSH (Daniel Stenberg, libcurl)
- ✿ 14.45 CyaSSL (Larry Stefonic, yaSSL)
- ✿ 15.00 Fribid and browser security software (Samuel Lidén Broell, [fribid.se](http://fribid.se))
- ✿ 15.30 EJBCA and OpenSC (Tomas Gustavsson, EJBCA)
- ✿ 16.00 Unifying access to PKCS#11 tokens (Nikos Mavrogiannopoulos, GnuTLS)
- ✿ 16.30 How to store trust: Trust assertions in PKCS#11 (Stef Walter, GnomeKeyring)
- ✿ 17.00 BOFH meets SystemTap: rootkits made easy (Adrien Kunysz)
- ✿ 17.30 Dynalogin: two factor authentication with HOTP (Daniel Pocock, Dynalogin)
- ✿ 18.00 OpenSC in 2015 - a look forward (Martin Paljak, OpenSC)
- ✿ 18.15 Open discussion panel - post your questions and ideas

# DISCUSSION PANEL

*“What **can** be done and what **should** be done to make using hardware cryptography devices with open source software a seamless experience for everyone?”*

- ✿ Continues 21:00 at a nearby restaurant, still some available seats.
- ☺ Big thanks to Aris for arranging the dinner!

**LET THE FUN BEGIN!**

**PROTECT YOUR PRIVATES!**