



FACULTY
OF INFORMATICS
Masaryk University

Java Card for KeePassXC

Adam Janovský, Marie William Gabriel Konan, Matěj Plch

KeePassXC

- password manager
- stores passwords in a database encrypted by password and/or keyfile
- one of many ports and forks of KeePass
- multiplatform
- written in C++ using Qt
- active development: 2000+ commits
- popular: 1200+ stars on GitHub
- <https://github.com/keepassxreboot/keepassxc>

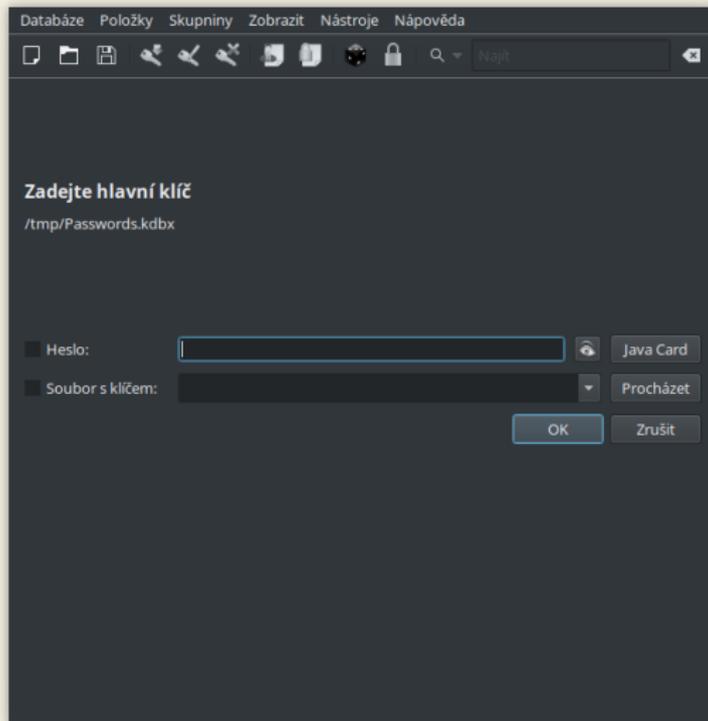
Java Card support

- add to KeePassXC button for requesting password stored on a card
- prompt user for a PIN
- fill in password field
- our public fork: <https://github.com/Afforix/keepassxc>
- using library PCSC-Lite for Java Card
- tested on Linux only
 - code should be multiplatform
 - PCSC-Lite basically is WinSCard
 - on Windows linking to PCSC-Lite may fail

Applet details

- PIN
 - length 4
 - applet locks after 3 unsuccessful attempts
- supported actions (APDUs):
 - authenticate by PIN
 - obtain password
 - set PIN
 - set password

Demo



Secure channel

- existing solution? - Global Platform
 - provides API for secure channel
 - existing C library without docs or examples
 - using security API without documentation is not secure!
- own solution? - asymmetric cryptography
 - key pair on the card, public key stored alongside the database
 - need to maintain integrity of the public key
- no secure channel implemented (yet?)
- any solution is insecure if initial setup is done over compromised channel