PV204 Security technologies

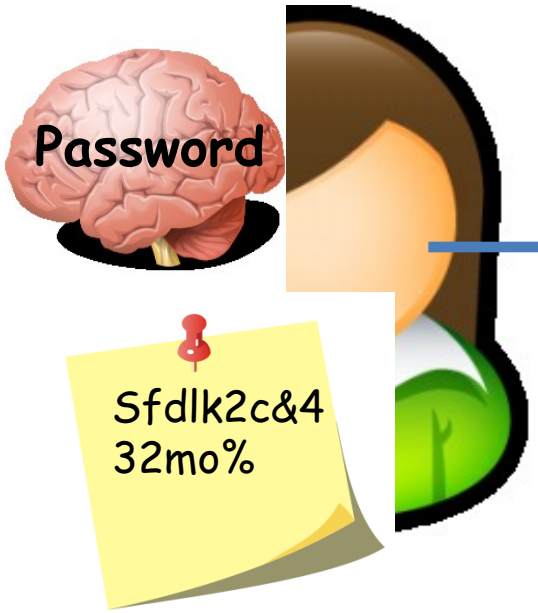
Team projects

Petr Švenda
Faculty of Informatics, Masaryk University, Brno, CZ

CROCS
Centre for Research on Cryptography and Security

Situation before your project

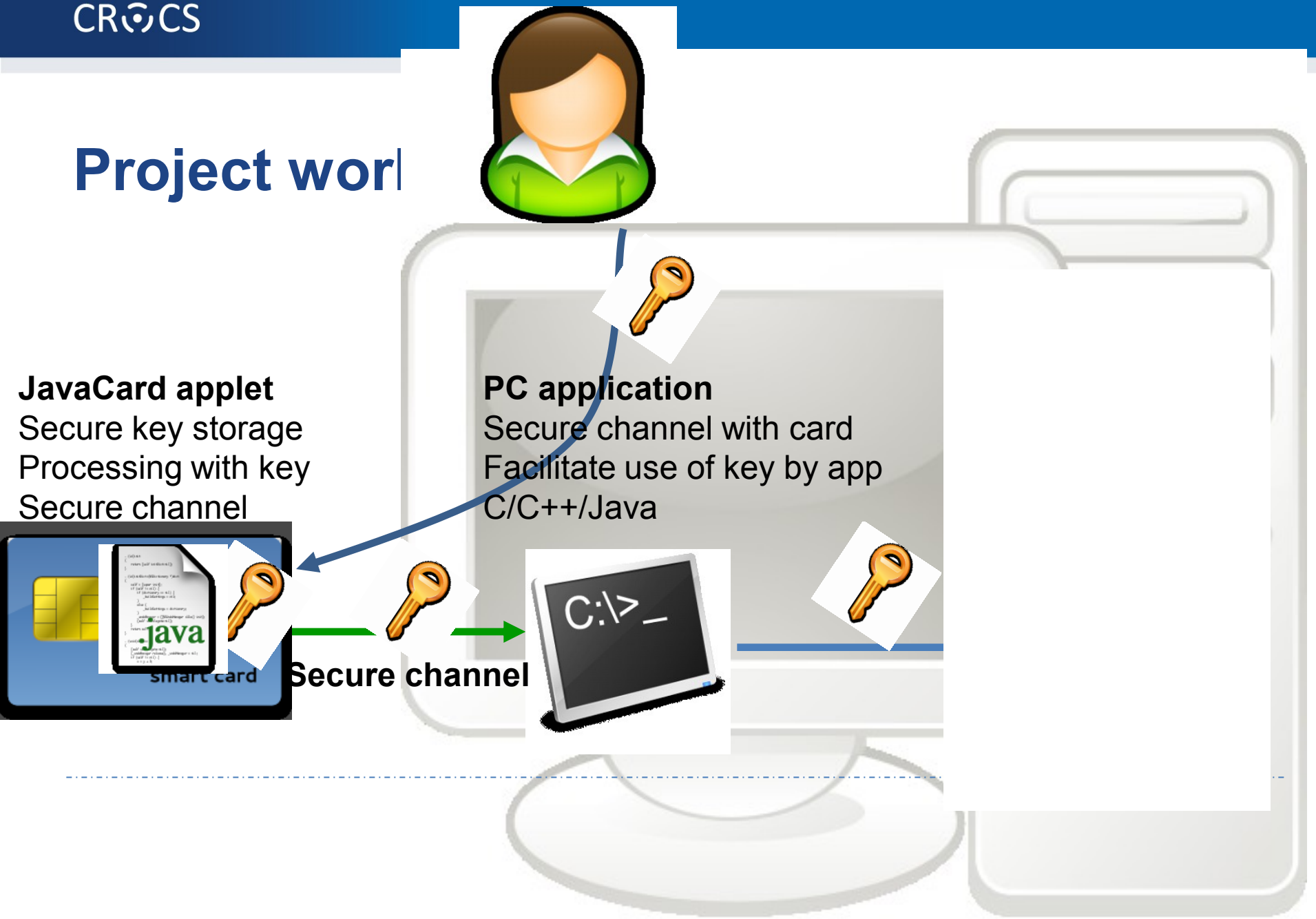
User stores keys
Memory, paper…



Key transmitted to PC app

Open-source application
password manager,
disk encryption,
zip encryption…

Project worl



Project

1. Identify suitable target scenario with need for cryptographic keys (disk encryption, remote authentication, DRM app…)
   - Open-source application
2. Design and implement JavaCard smart card applet
   - Storage and processing of secrets (keys)
   - Authentication and secure channel with PC application
   - Source code and installation scripts provided to other teams (code review)
3. Design and implement PC-based counterpart application
   - Establish secure channel with smart card applet
   - Transmit key from card or transmit data for processing
4. Review implementations of other teams
   - Review design choices made by other team
   - Review source code of other team applet and application (just newly added parts)

Teams

- 3 people per team
  - Assigned today (within group), available in IS
- Teams must use GitHub for cooperation
  - Distribute work load between all members
  - Contribution from all team members must be visible in commits (git commits from the member)
  - Your evaluation will be partially based on your participation
- Start working early, especially with implementation
- Teams may use own existing code from previous assignments (SimpleApplet etc.)

Projects - timeline

1. Identify target scenario, design of applications: 3 points ~~(6.4.2017)~~
   - Report (max. 2 pages A4)
   - Deadline moved to 11.4.
2. Write code (GitHub): 10 points (before 4.5.2017)
   - JavaCard application, PC-based application
   - Design, code + presentation ~~(4.5.2017~~, your seminar group, random team member) – presentation moved to 27.4.
3. Review and attack implementations: 7 points (before 18.5.2017)
   - Up to 4 points assigned by reviewers, up to 3 points by me
   - Review and attack implementations of other teams
   - Report + presentations (18.5.2017, random team member)

- At least 10 points (total) from project are required