PV204 Project – Phase 2

IMRICH NAGY & DANIEL RYCHLÝ

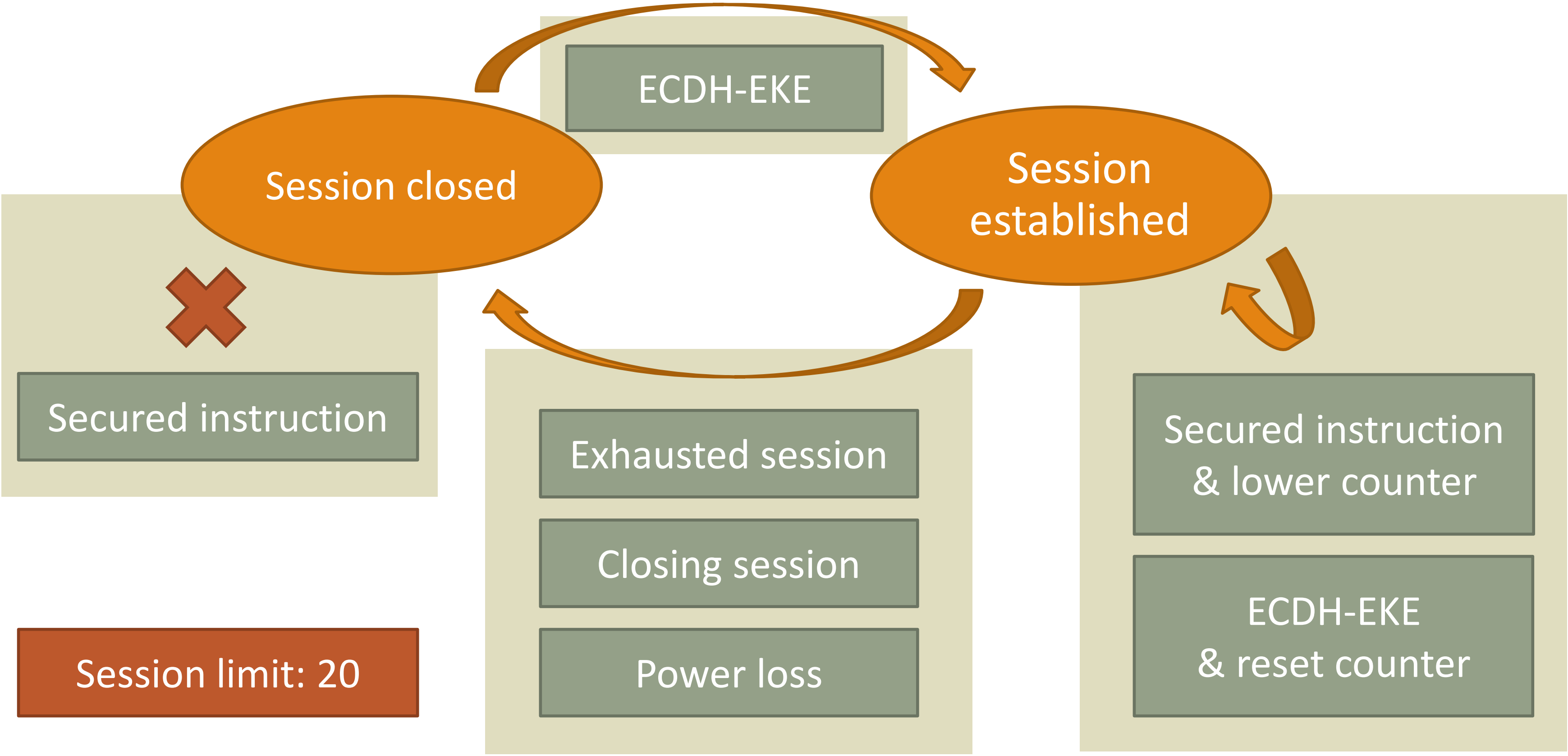
Overview

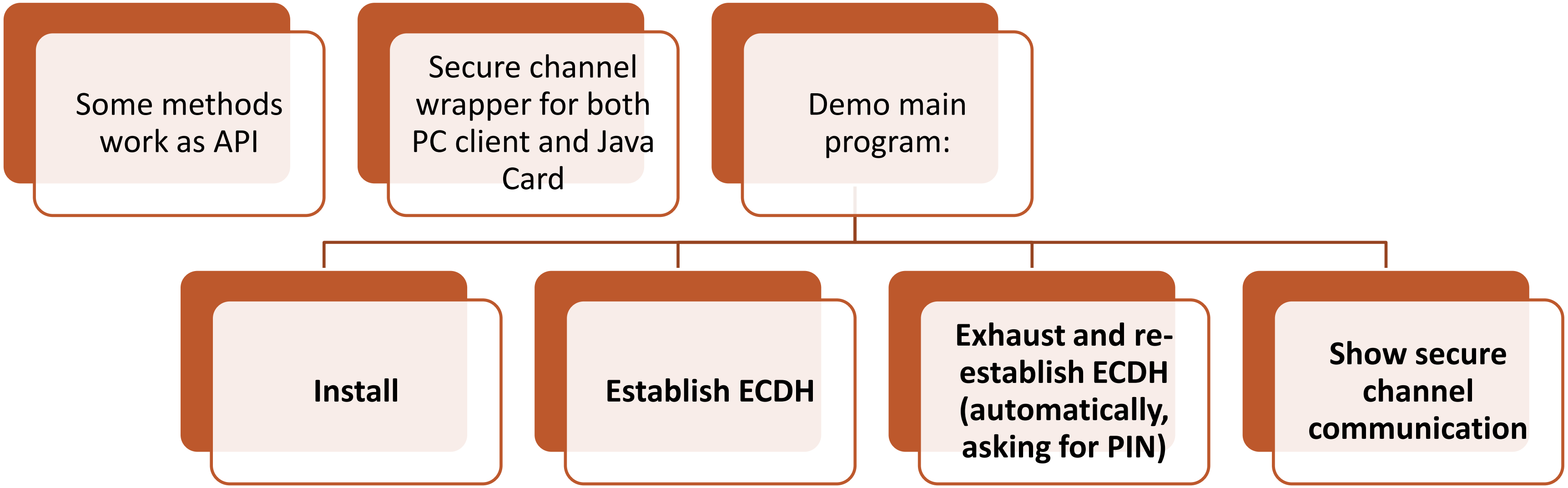
- PIN installed during applet installation
- Ephemeral ECDH authenticated by PIN
- Session keys derived from shared ECDH secret
- Every incoming/outgoing data encrypted
- Session end

Secure channel encryption

- 128-bit AES in CBC mode with IV derived along with the key
- PKCS#5 padding used (unsupported in the JCardSim, implemented)
- Cipher.update() not working properly
- Key and IV swapped in one way

Secure channel (automata-based programming)





Some methods work as API

Secure channel wrapper for both PC client and Java Card

Demo main program:

Install

Establish ECDH

Exhaust and re-establish ECDH (automatically, asking for PIN)

Show secure channel communication

The demo program

Project work

- Only two team members
- Used Card Tools provided by PetrS
- Complete documentation
- Documented demo program, no tests
- GitHub branches, projects, milestones, issues
- Commented APDU traces in report
- About 50 hours per team member

Some details worth mentioning

Tried to use as little ROM as possible

Cipher.OneShot not implemented in JCardSim?

Almost no ANSI X9.62 encoding function anywhere

Ease of addition of new instructions

THANK YOU

Hand the word over to Dan