MTAT.07.017
Applied Cryptography

Rakenduslik krüptograafia
Прикладная криптография

Juri Hudolejev
University of Tartu
Spring 2011

Topic for This Week

Smart Cards

Java Smart Card API vs Java Card

`javax.smartcardio.*`

Smart Card

Card with integrated circuits (ICC)

Non-volatile memory only

- Storage media

Memory and microprocessor

- Standalone computer

Smart Card as a Computer

CPU: 8-bit 3.5 MHz … 32-bit 32 MHz

RAM: 4 … 32 KB

ROM: 64 … 256 KB

EEPROM/Flash 1 … 256 KB

640 KB is enough for anyone

http://smartcardbasics.com/smart-card-types.html

4.77 MHz / 64 KB RAM

1983

Smart Cards by Form Factor

85.60 x 53.98 – ISO/IEC 7810 ID-1 (CR80)

Most banking, ID and contactless cards

25 x 15 – Mini-SIM

15 x 12 – Micro-SIM

Flash cards – CF, MS, PCMCIA, SD, xD

Smart Card Usage

Identification, authentication, access control

Secure data storage

Application processing

- Payments
- Cryptography

Smart Card Life Cycle

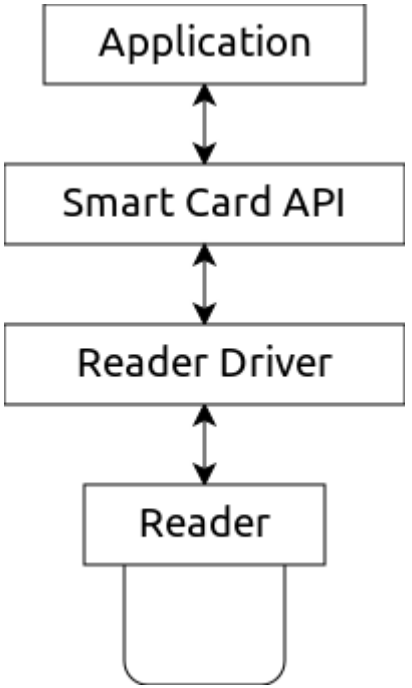
Manufacturing – assembling the hardware

Initialization – installing the middleware

Personalization – installing the applications

Usage – running the applications

Working with Smart Cards



Working with Smart Cards

Application (DigiDoc client, payment app, ...)

- (PKCS#11, Crypto API, CDSA, ...)

Smart card API (OpenSC, Java SC API, ...)

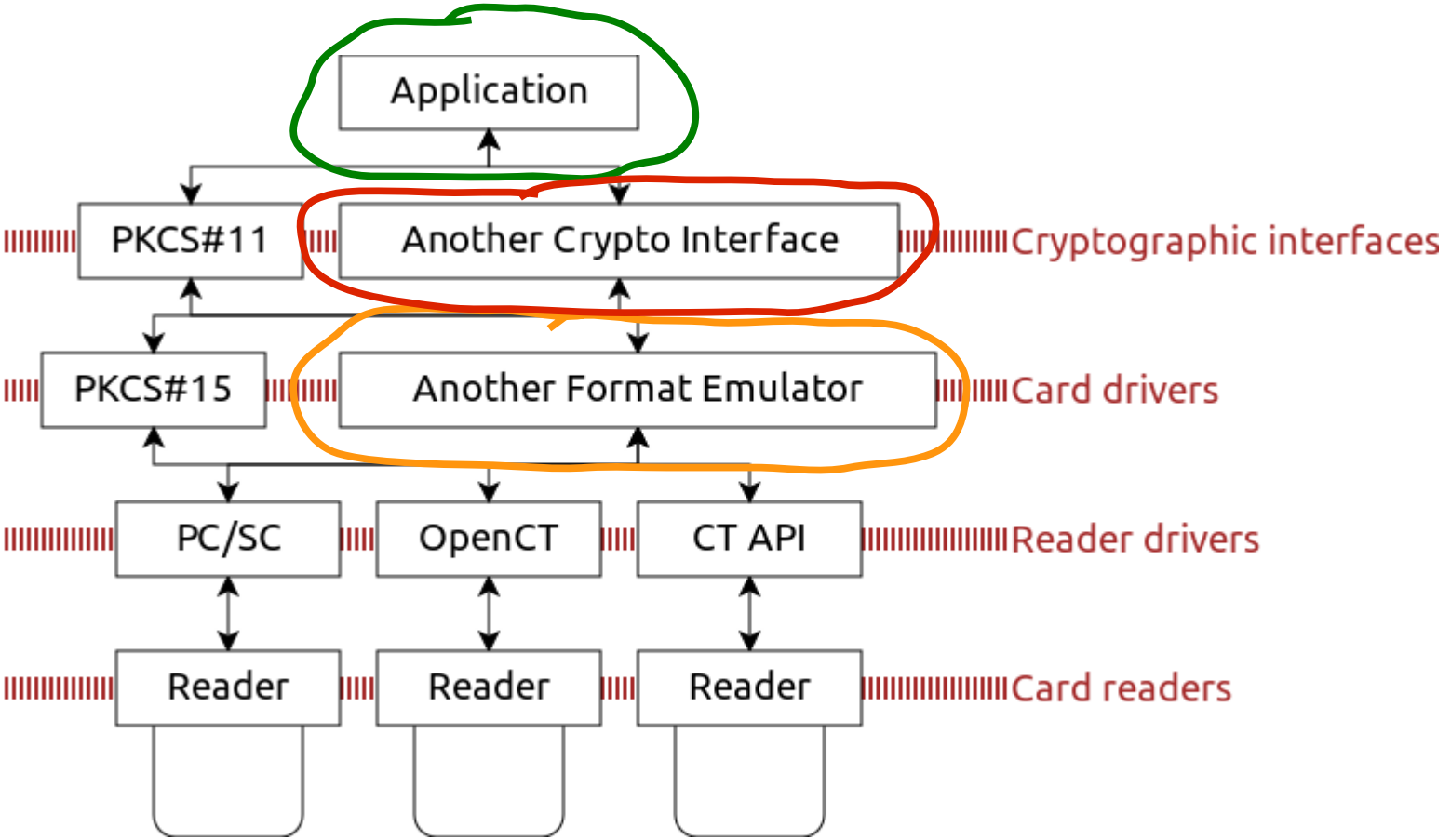
- (PKCS#15, ...)

Smart card reader driver (PC/SC, CT API, ...)

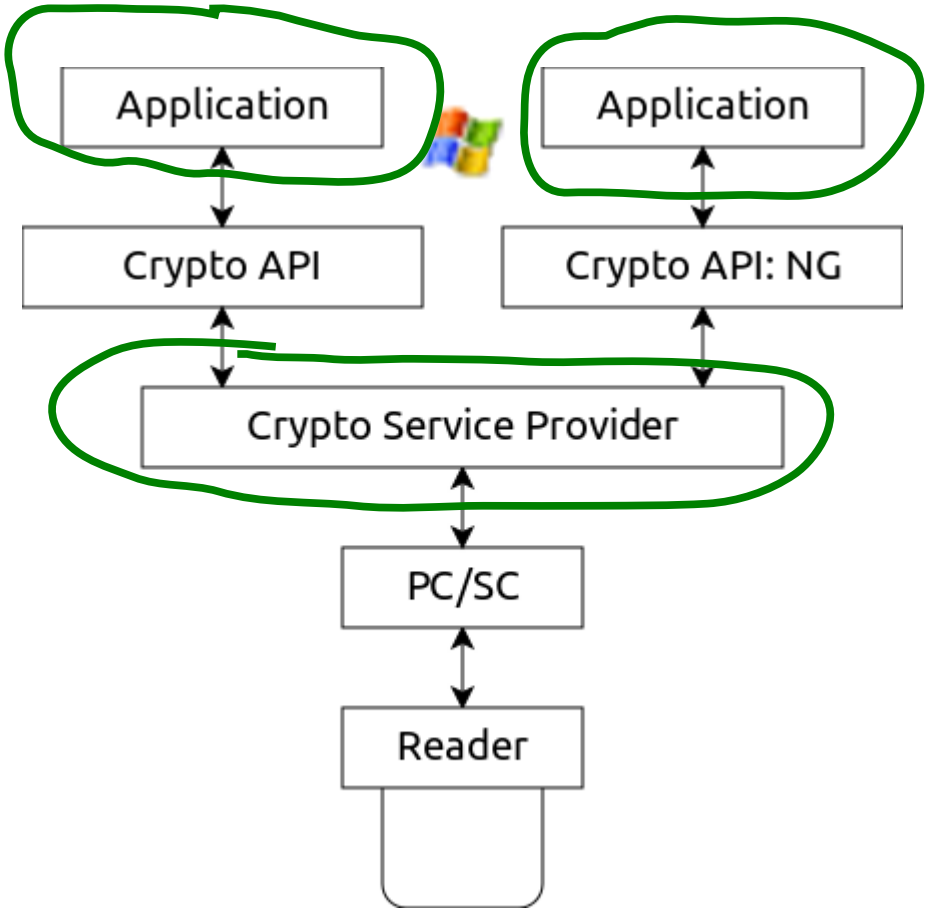
- (USB, serial, PCMCIA, IR...)

Smart card reader ⇔ Smart card

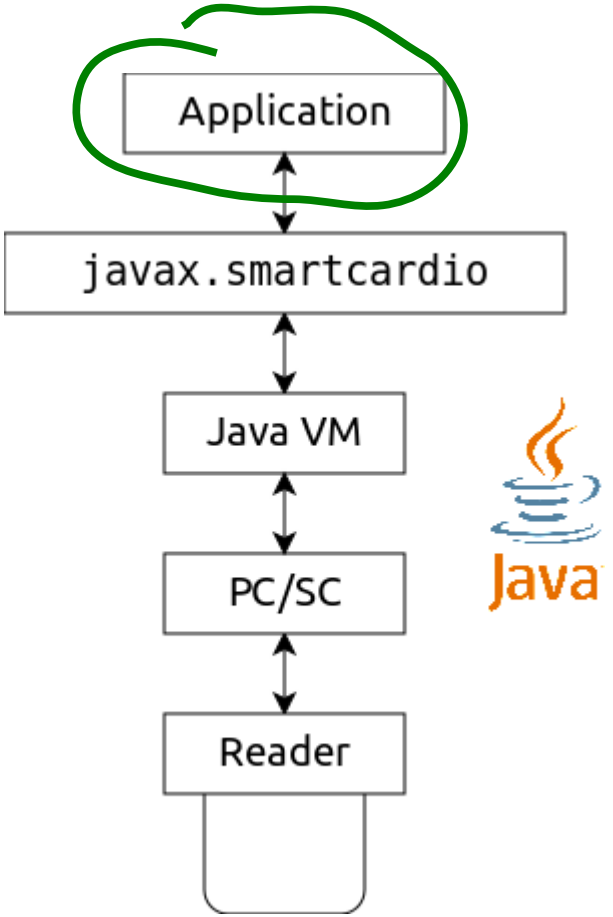
Working with Smart Cards



Working with Smart Cards



Working with Smart Cards



Smart Card Communication

Smart card resources are **very** limited –

cannot store any libs or interfaces... Yet.

APDU: Application Protocol Data Unit

terminal → card: command APDU

card → terminal: response APDU

Command APDU

Header (4 bytes) + data (0 … 255 bytes)

```
[CLA][INS][P1][P2][L_C][C]...[L_E]
```

Examples:

```
00 b2 01 0c ff
00 a4 01 0C 02 ee ee 00
```

Response APDU

Data (0 … 256 bytes) + status word (2 bytes)

```
[R]...[SW1][SW2]
```

Examples:

```
6a 82
45 53 54 90 00
```

Smart Card Specifications

ISO/IEC 7810 – card physical characteristics

ISO/IEC 7816 – formats and protocols

EMV – Europay-MasterCard-VISA

beID, CIE, DigiD, EstEID, …

Java Card

Technology to run applets on smart cards

- Standard Java app: write once – run on every OS (ideally)
- Smart card app: write once – run on every card

Goal: standard smart card environment

- Very basic Java VM on smart card

More examples:
http://www.opensc-project.org/opensc/wiki/JavaCard

Further Reading

~ http://en.wikipedia.org/wiki/Smart_card

http://www.smartcardbasics.com/

http://www.opensc-project.org/

http://emvco.com/specifications.aspx?id=155

http://id.ee/?id=10457

Questions?

0x9000

Homework: none for this week

Deadline for lab 10 tasks:

2011-05-13 **08:00** EEST

Next lab session:

Friday 2011-05-13 **08:30** EEST @ Liivi 2 - 205