PB173 - Tématický vývoj aplikací v C/C++ (jaro 2016)

Skupina: Aplikovaná kryptografie a bezpečné programování

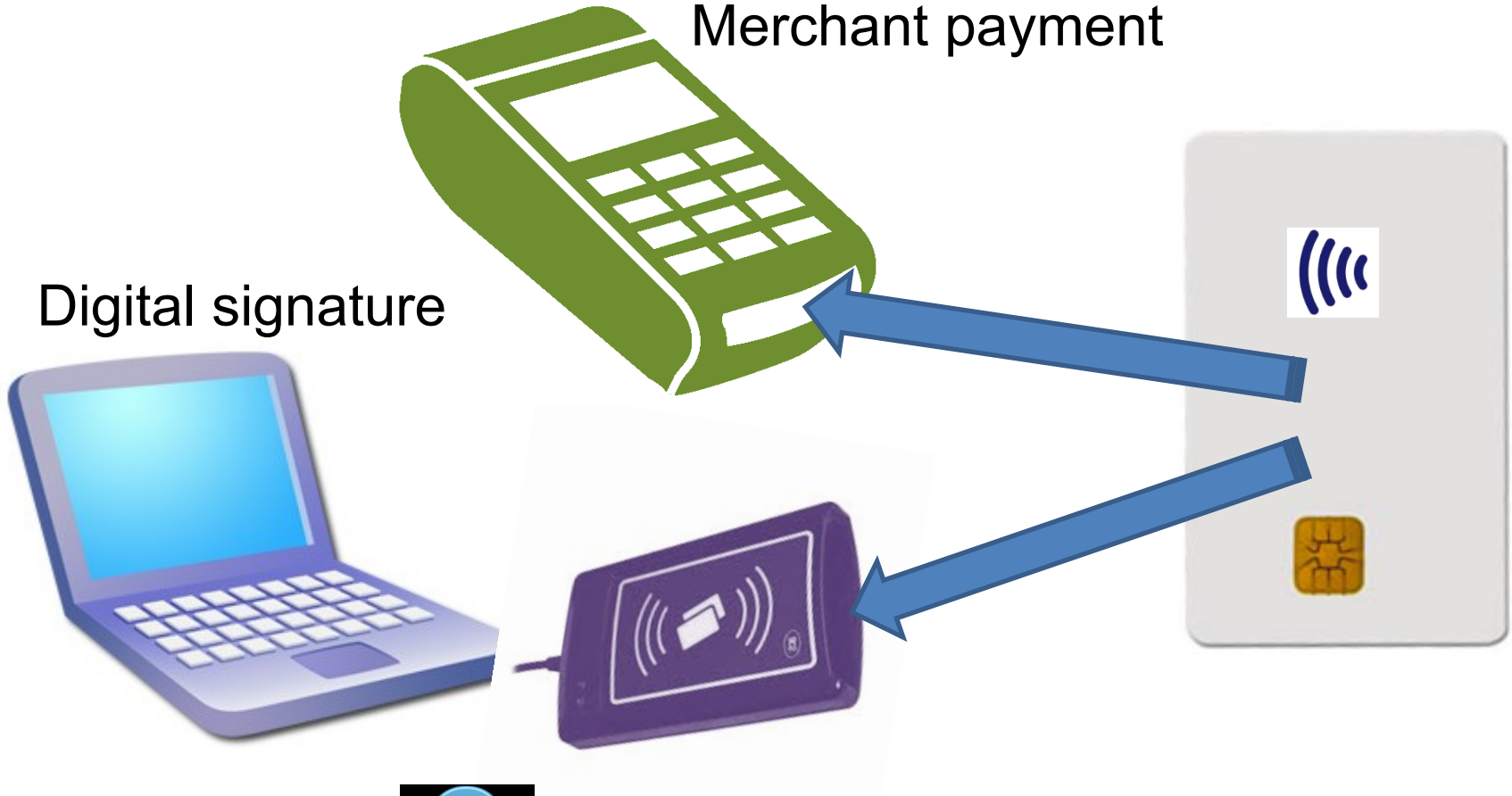
Petr Švenda svenda@fi.muni.cz

Konzultace: A.406, Pondělí 15-15:50

CROCS
Centre for Research on Cryptography and Security

SMARTCARDS IN WIDER SYSTEM

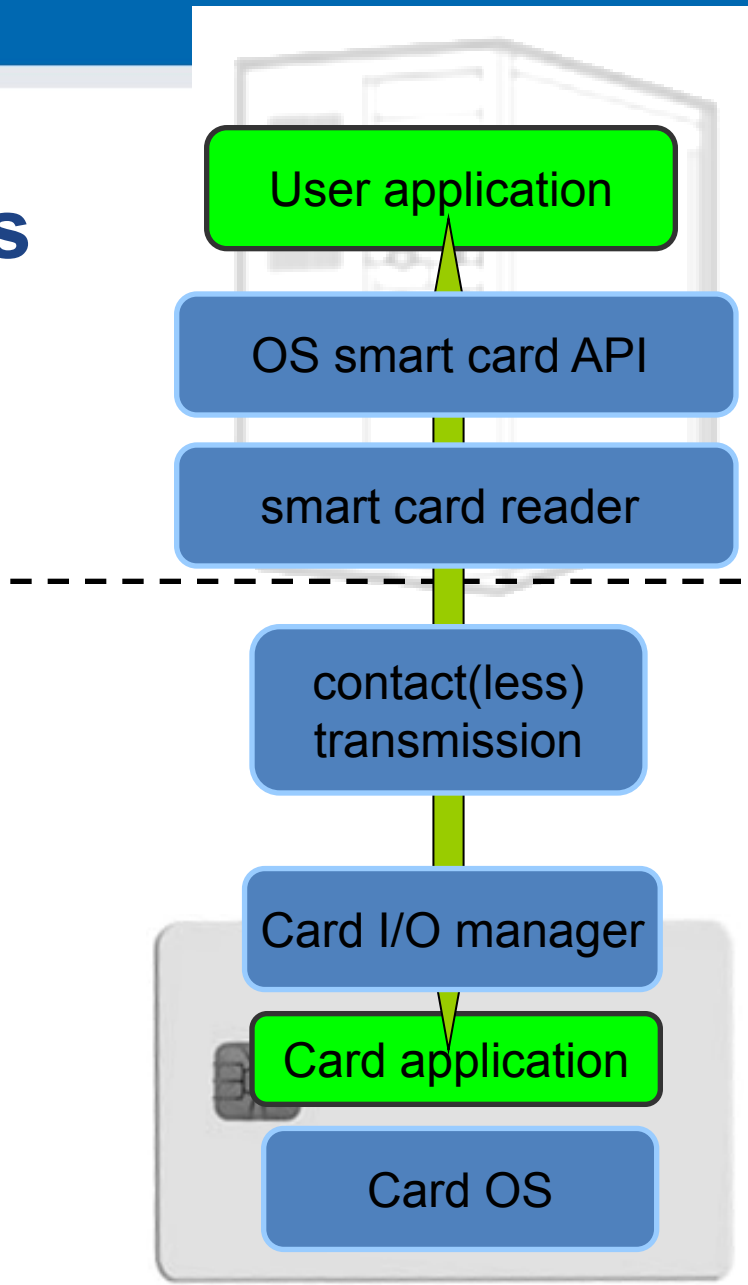
Big picture – terminal/reader and card

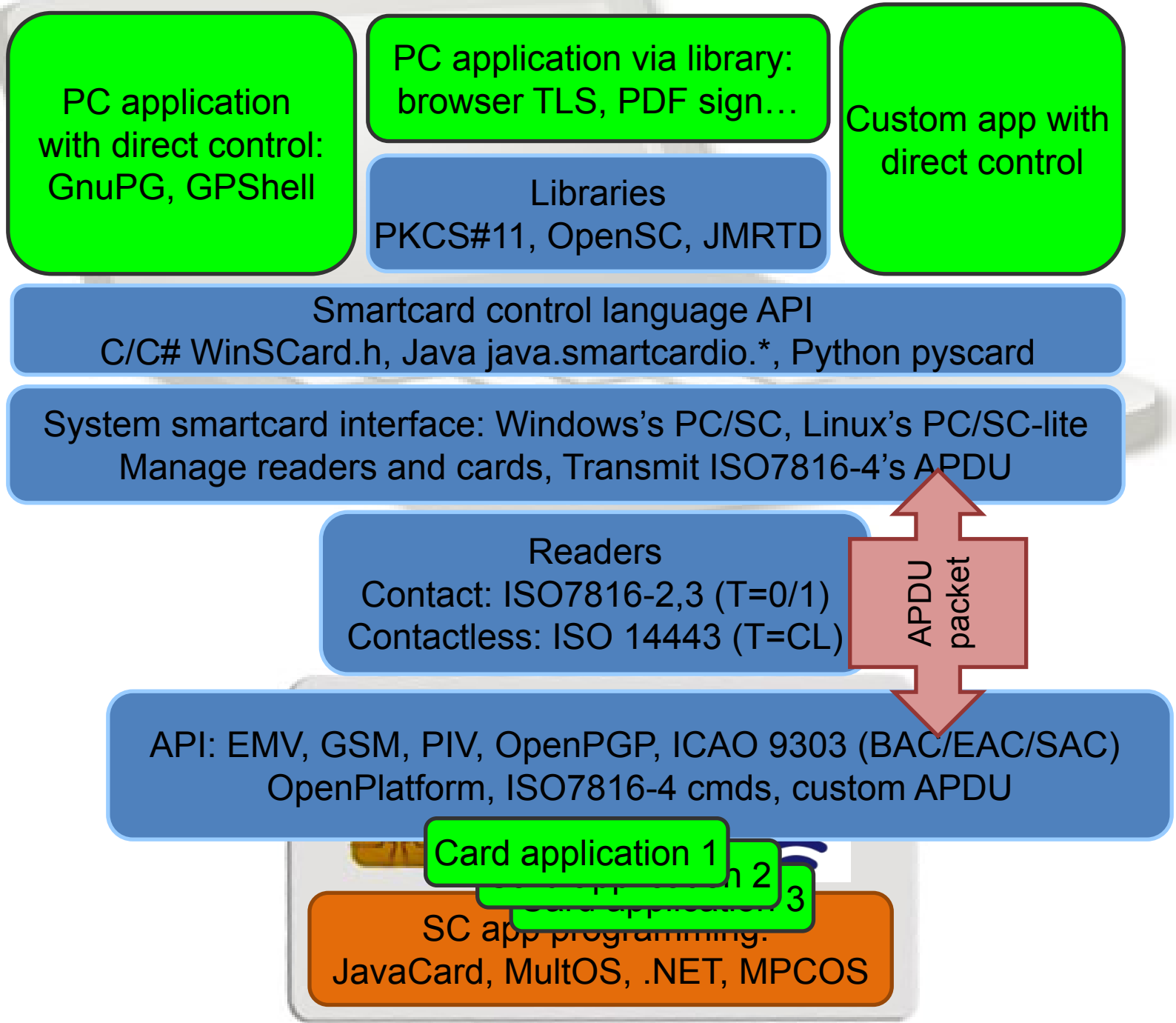


What principles and standards are used?

Big picture - components

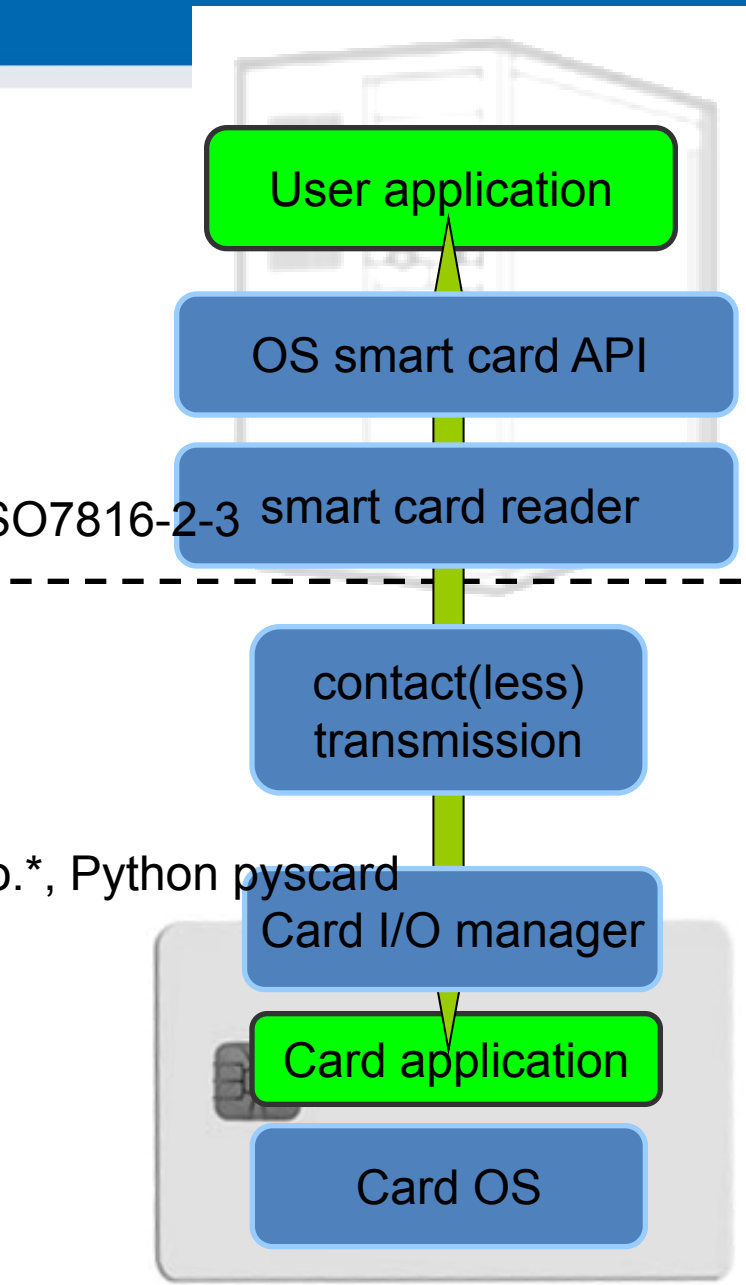
- User application
  - Merchant terminal GUI
  - Banking transfer GUI
  - Browser TLS
  - …
- Card application
  - EMV applet for payments
  - SIM applet for GSM
  - OpenPGP applet for PGP
  - …




PC application with direct control: GnuPG, GPShell
PC application via library: browser TLS, PDF sign…
Custom app with direct control
Libraries
PKCS#11, OpenSC, JMRTD
Smartcard control language API
C/C# WinSCard.h, Java java.smartcardio.*, Python pyscard
System smartcard interface: Windows's PC/SC, Linux's PC/SC-lite
Manage readers and cards, Transmit ISO7816-4's APDU
Readers
Contact: ISO7816-2,3 (T=0/1)
Contactless: ISO 14443 (T=CL)
APDU packet
API: EMV, GSM, PIV, OpenPGP, ICAO 9303 (BAC/EAC/SAC)
OpenPlatform, ISO7816-4 cmds, custom APDU
Card application 1
SC app programming:
JavaCard, MultOS, .NET, MPCOS

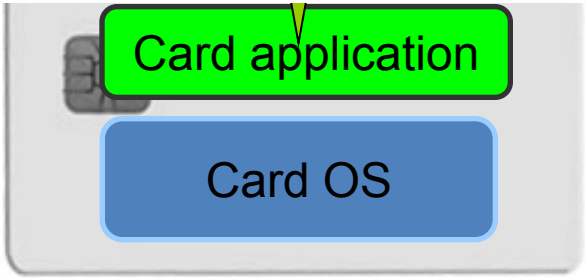
Main standards

- ISO7816 1-4
  - Card physical properties ISO7816-1
  - Physical layer communication protocol ISO7816-2-3
  - Data packet format (APDU)
- PC/SC, PC/SCLite (host side)
  - Readers/cards management
  - Transmission of logical APDU packets
  - C/C# WinSCard.h, Java java.smartcardio.*, Python pyscard
- PKCS#11
  - standardized interface on host side
  - card can be proprietary
- GlobalPlatform
  - remote card management interface
  - secure installation of applications



Card's programming platforms

- MultOS
  - Multiple supported languages, native compilation
  - Often bank cards
- JavaCard
  - open programming platform from Sun
  - applets portable between cards
- Microsoft .NET for smartcards
  - Similar to JavaCard, but C#
  - Applications portable between cards
  - Limited market penetration



What is the typical performance?

- Hardware differ significantly
  - Clock multiplier, memory speed, crypto coprocessor…
- Typical speed of operation is:
  - Milliseconds (RNG, symmetric crypto, hash)
  - Tens of milliseconds (transfer data in/out)
  - Hundreds of millisecond (asymmetric crypto)
  - Seconds (RSA keypair generation)

- Operation may consists from multiple steps
  - Transmit data, prepare key, prepare engine, encrypt
  - → additional performance penalty

Performance tables for common cards

- Visit http://www.fi.muni.cz/~xsvenda/jcalgtest/

CARD/FUNCTION (ms/op)	SECURE RANDOM (256B)	SHA-1 hash (256B)	SHA2-256 hash (256B)	3DES encrypt (256B)	AES128 encrypt (256B)	AES256 encrypt (256B)	3DES setKey(192b)	AES setKey(128b)
Gemplus GXP R4 72K	2.45	3.69	-	53.71	26.05	31.52	9.4	9.28
NXP JCOP 31 V2.2 36K	6.92	19.84	-	7.27	-	-	26.1	-
NXP JCOP 21 V2.2 36K	7.28	20.91	-	7.68	-	-	25.84	-
NXP JCOP41 v2.2.1 72K	7.58	21.77	-	8.02	-	-	15.44	-
NXP J2D081 80K	10.4	11.73	21.18	7.1	6.73	7.66	20.12	16.31
NXP CJ3A081	13.8	11.45	21.05	12.8	10.33	11.35	11.04	10.9
NXP JCOP CJ2A081	14.14	11.9	22.46	13.3	10.78	11.81	5.39	5.22
NXP J2A080 80K	19.59	31.09	60.16	18.11	18.57	20.12	12.24	11.91
NXP JCOP31 v2.4.1 72K	20.97	34.1	66.02	19.95	20.44	22.24	6.7	6.38
NXP J3A080	21.64	35.78	69.32	20.92	21.41	23.2	15.48	12.28
Infineon CJTOP 80K INF SLJ 52GLA080AL M8.4	24.9	17.42	35.58	61.49	25.53	31.18	6.61	6.08
NXP JCOP21 v2.4.2R3	33.77	12.35	22.39	12.24	11.65	14.02	31.35	23.48
Oberthur ID-ONE Cosmo 64 RSA v5.4	52.49	23.53	-	16.05	-	-	25.31	-
G+D Smart Cafe Expert 4.x V2	322.91	33.66	-	37.19	-	-	3.59	-

Practical assignment (from last week)

- Client to client network communication
- Speed-up encryption of data packets between two clients with CTR mode
  - Divide packet into multiple parts
  - Use parallel threads to protect parts of data packet
    - number of available cores is parameter for function
    - (at least one thread required ;))
- Document performance gains
  - speed before and after the optimization (can you increase speed linearly?)
  - What is length of packet for which multiple threads brings speedup benefit? (overhead with running threads)

Submissions, deadlines

- Upload application source codes as single zip file into IS Homework vault (Crypto - 8. homework (Threads))
- DEADLINE 2.5. 12:00
  - 0-10 points assigned