

Laboratorium

Programowania Kart Elektronicznych

Interfejs bezkontaktowy, Mifare

Marek Goławski

Interfejs bezkontaktowy, Mifare

- Przygotowanie do zajęć
 - sprawna legitymacja studencka
 - otrzymane od prowadzącego karty Mifare
- Potrzebne wiadomości
 - język angielski w stopniu pozwalającym na czytanie dokumentacji technicznej
 - arytmetyka szesnastkowa

Interfejs bezkontaktowy, Mifare

- Oprogramowanie
 - przykładowe programy otrzymane razem z bibliotekami do czytnika (Omnikey, Samples)
 - *contactlessdemovb*
 - *contactlessdemovc* (release)
 - EasyReader
 - SmartCardSuite (zastępuje funkcje powyższych)
 - <http://sourceforge.net/projects/smartcardsuite/>
 - mile widziane wszelkie informacje o błędach, pomysły

„Słowniczek”

- **Mifare**

- standard przemysłowy – omówiony dalej

- **PEKA**

- Poznańska Elektroniczna Karta Aglomeracyjna,

- <http://www.peka.poznan.pl/>

Interfejs bezkontaktowy, Mifare

- Zadania
 - odczytanie UID legitymacji studenckiej
 - przedstawienie w postaci dziesiętnej „wprost” i „wspak”
 - znalezienie w pamięci Mifare tekstu „LabPKE”
 - UID karty oraz numer bloku i sektora
 - omnikey samples, contactlessdemovc
 - EasyReader
 - podanie numeru karty bibliotecznej
- Przesłanie na adres:
 - marek.goslowski@put.poznan.pl

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- ELS w systemie kontroli dostępu 😊
 - system „on-line”
 - po zgłoszeniu w eStudent/eKD
 - <https://ekd.put.poznan.pl/>
 - wjazd na teren PP, dostęp do „rowerowni”
 - **ważna legitymacja studencka (przedłużona)**
 - po zgłoszeniu przez „operatora”
 - wejście do akademika

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- Zastosowania ELS

- karta miejska

- KOMKarta – Mifare 1K
 - PEKA – ISO 14443, T=CL

- karta płatnicza (PayPass, VPay)

- karta biblioteczna (jELIB)

- *programy lojalnościowe*

<http://www.mcp.poznan.pl/funkcje-karty-els/>

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- Standard przemysłowy
 - dawniej Philips, teraz NXP
 - MF1ICS50 Functional specification (Mifare 1K)
 - *RFID Cooking with Mifare Classic*
 - *Proxmark III*
 - ...
- ISO/IEC 14443 Type A
- 13,56 MHz (m.in. NFC!)

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- Organizacja pamięci
 - sektory: 16 (0-15)
 - bloki: 64 (0-63),
4 bloki / sektor

		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A					Access Bits					Key B					Sector Trailer 15	
	2																	Data
	1																	Data
	0																	Data
14	3	Key A					Access Bits					Key B					Sector Trailer 14	
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A					Access Bits					Key B					Sector Trailer 1	
	2																	Data
	1																	Data
	0																	Data
0	3	Key A					Access Bits					Key B					Sector Trailer 0	
	2																	Data
	1																	Data
	0																Manufacturer Block	

Fig 4. Memory organization

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- sektor 0, blok 0
 - numer seryjny (UID)
 - 4/7/10 bajtów
- każdy sektor, blok 3
 - klucze
 - uprawnienia

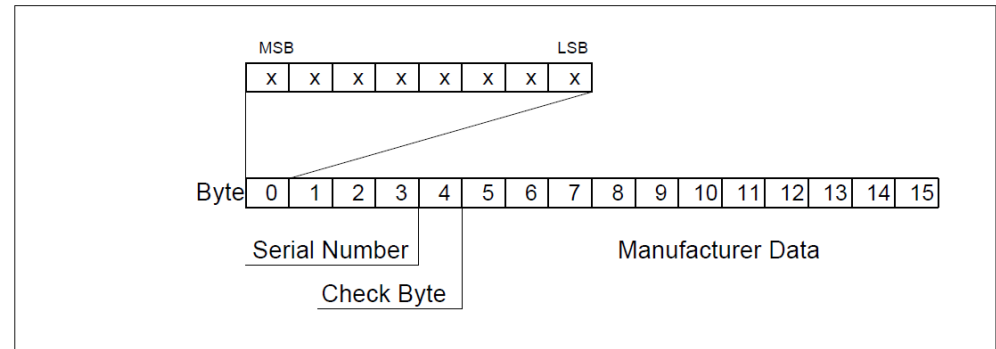


Fig 5. Manufacturer block

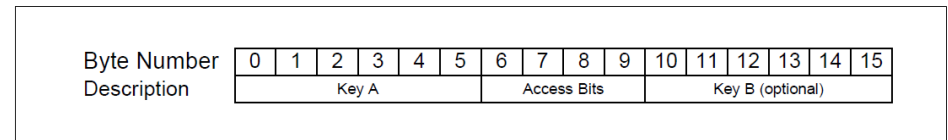


Fig 7. Sector trailer

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

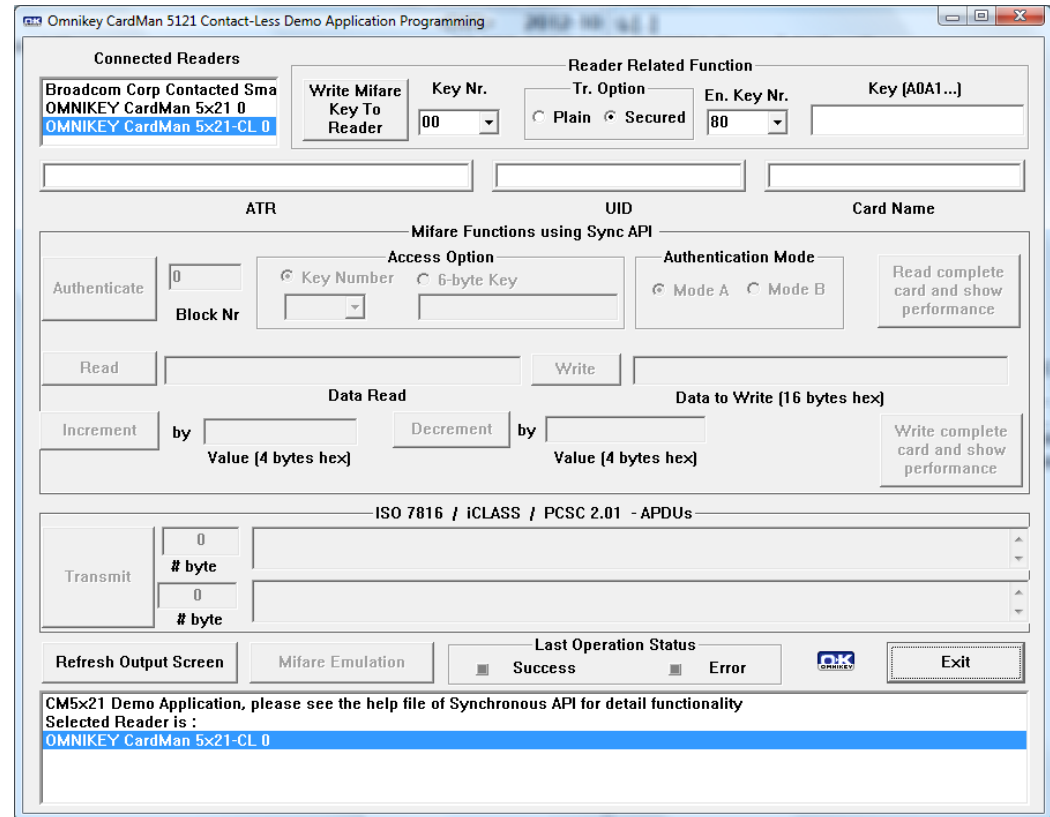
Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- Authenticate
- Read/Write
- Mifare emulation
- Keys
 - A: FF FF FF FF FF FF,
 - B: FF FF FF FF FF FF



Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

marek.goslowski@put.poznan.pl

Interfejs bezkontaktowy, Mifare

- Czytniki omnikey,
 - przełączenie trybu działania czytnika, regedit
 - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CardMan\RFID**
 - **ControlFlags=0x00000004**
 - » OMNIKEY's host-side MIFARE emulation ON default
 - **ControlFlags=0x00000000**
 - » OMNIKEY's host-side MIFARE emulation OFF T=CL, for on-card MIFARE emulation
 - „restart” czytnika

Interfejs bezkontaktowy, APDU

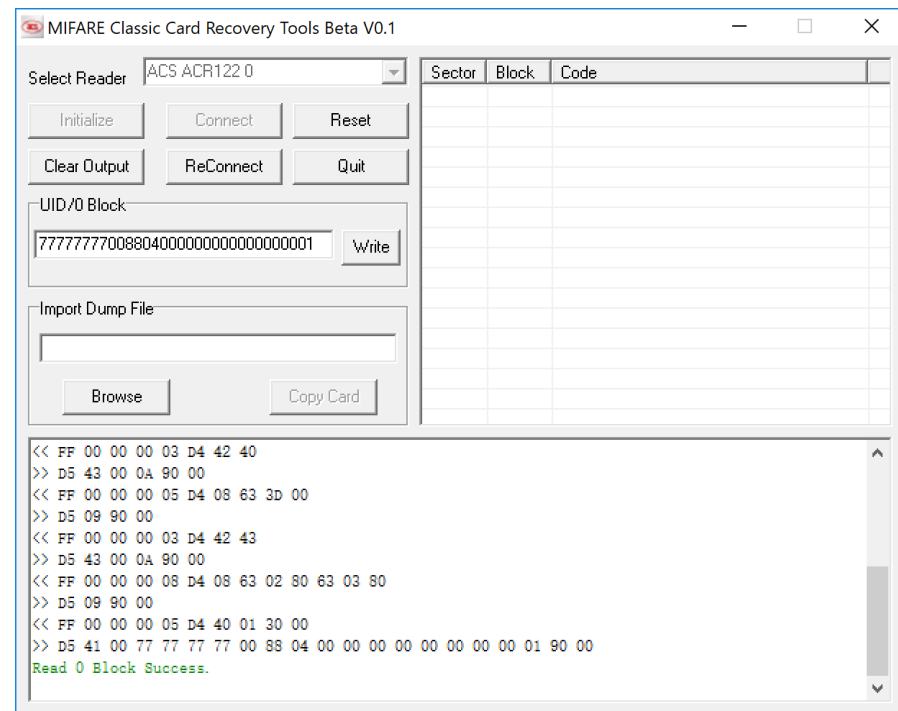
- PS/SC, część 3 (Requirements for PC-Connected Interface Devices)
- Polecenia (APDU)
 - Get Data (UID)
 - **FF CA 00 00 00**
 - Get Data (historical)
 - **FF CA 01 00 00**
 - Load Keys
 - **FF 82 20 00 06 FF..FF**

Interfejs bezkontaktowy, APDU

- Polecenia (APDU)
 - General Authenticate
 - **FF 86 00 00 05 <data>**
 - Read Binary
 - **FF B0 00 00 10|00**
 - Update Binary
 - **FF D6 00 00 XX <data>**
 - Increment, Decrement, Verify

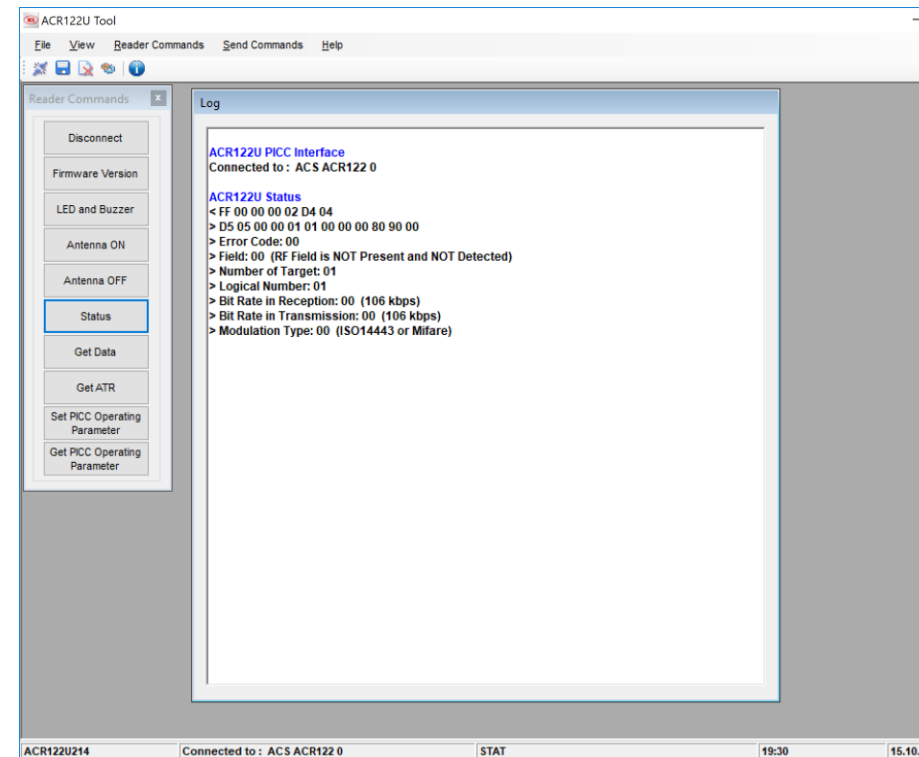
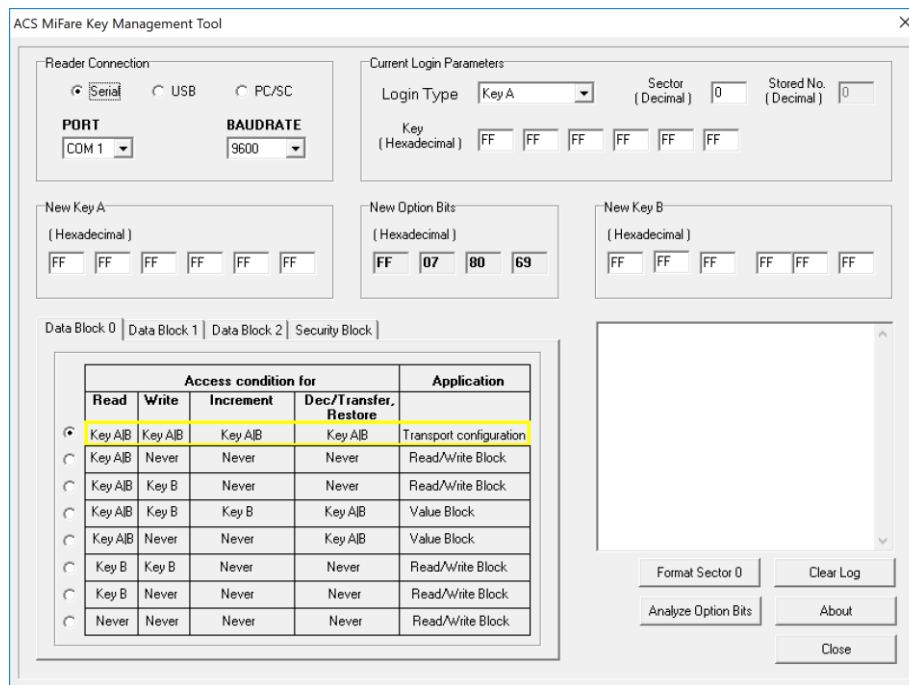
Interfejs bezkontaktowy, ACR122

- Sprzęt
 - czytnik ACR122
 - karty ze zmiennym UID
 - „specjalne” oprogramowanie



Interfejs bezkontaktowy, ACR122

- Oprogramowanie podstawowe
 - ACR Tool
 - EasyKey



Interfejs bezkontaktowy, jELIB

- jELIB (*omnikey, przełączenie trybu działania czytnika, regedit*)
 - AID: D6 16 00 00 40 01 01
 - <http://www.mcp.poznan.pl/oprogramowanie/jelib/>
 - przykłady poleceń ded. w pracy dyplomowej
 - C0 39 00 00 00
 - C0 31 01 00 04 54 02 01 01 00
 - C0 33 01 01 03 52 01 02 00
 - C0 33 02 00 06 51 04 50 46 42 4E („PFBN”)

Zadanie 1: odczytanie UID legitymacji studenckiej

Zadanie 2: znalezienie w pamięci Mifare tekstu „LabPKE”

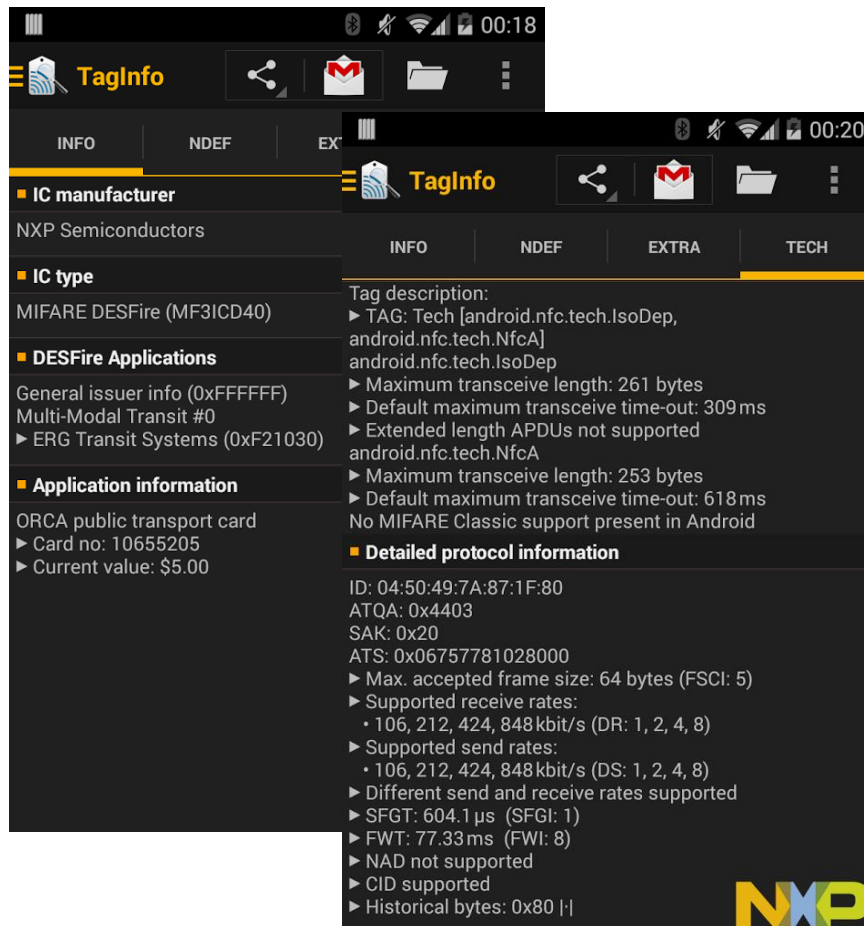
Zadanie 3: podanie numeru karty bibliotecznej

wysłać na adres:

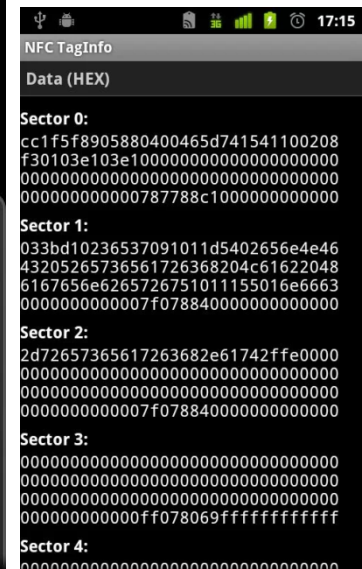
marek.goslowski@put.poznan.pl

Inne oprogramowanie (android)

- NFC TagInfo by NXP



- NFC TagInfo
- PassportImageDecoder



3:05

EMV Paycard Reader

CARD DETAIL

TRANSACTIONS

LOG

Card Representation

Bank

4123 4567 8901 2345

Expire 08/14

VISA

Extended card details

Holder name : John Doe

Card AID : A0 00 00 00 03 10 10

Application : CB

Card type : VISA

Pin try left : 3 Time(s)

Card issuer : CB Visa Banque Populaire (France)
(possible)

- The screenshot shows the 'Mifare Classic Tool' application. The top status bar displays the time as 13:31. The app's main menu includes 'Read Tag', 'Write Tag', 'Edit/Analyse Dump File', 'Edit/Add Key F', 'Tools', and 'Help and Info'. The 'Dump Editor' section is open, showing hex data for four sectors. The data is color-coded: green for UID and MANUF, blue for VALUE BLOCK, yellow for KEY A, red for KEY B, and purple for ACS. The app version is 1.0.0.

Mifare Classic Tool

Read Tag

Write Tag

Edit/Analyse Dump File

Edit/Add Key F

Tools

Help and Info

Dump Editor

Sector: 0

5270BB4CC1880400C185149151201011
01020304050000000090A0B0C0D0E08079
091111120011201CB422C9F1707660880
FFFFAABCCDD63C78900FF0011BB8888

Sector: 1

1E000000E1FFFFFF1E00000000FF00FF
00000000000000000000000000000000
0000000000000000000000000000AABB
00112233445540F78B00A0A1A2A3A4A5

Sector: 2

20FF110C07DC0C3FFF0001F400000009
264D120307DD0D0A0000000000001234
3d2048656c6c6f20576f726c64203d00
00000000000072D78800-----

Sector: 3

AABBCDDDEEFF00112233445566778899
FD829385BBBB0000000000000000A0A
0000999992123000000000000000FF
FFAAFFAAFFAA70F788001111111111FF

Sector: 4

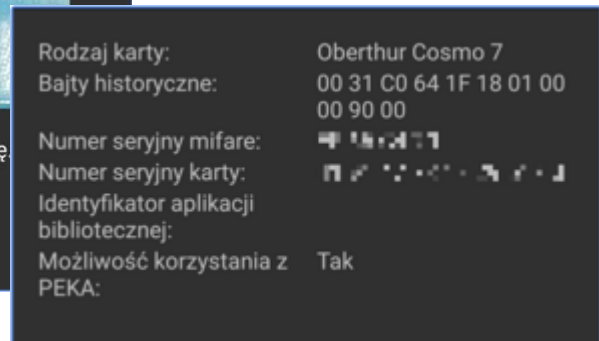
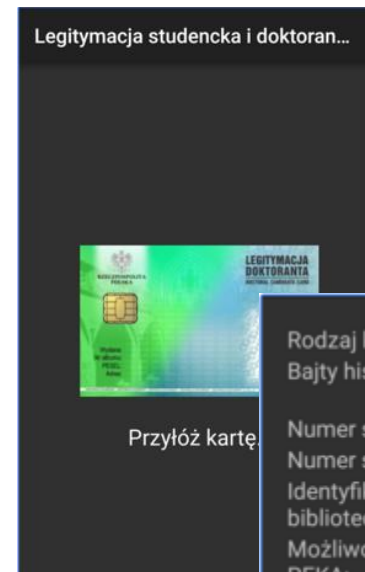
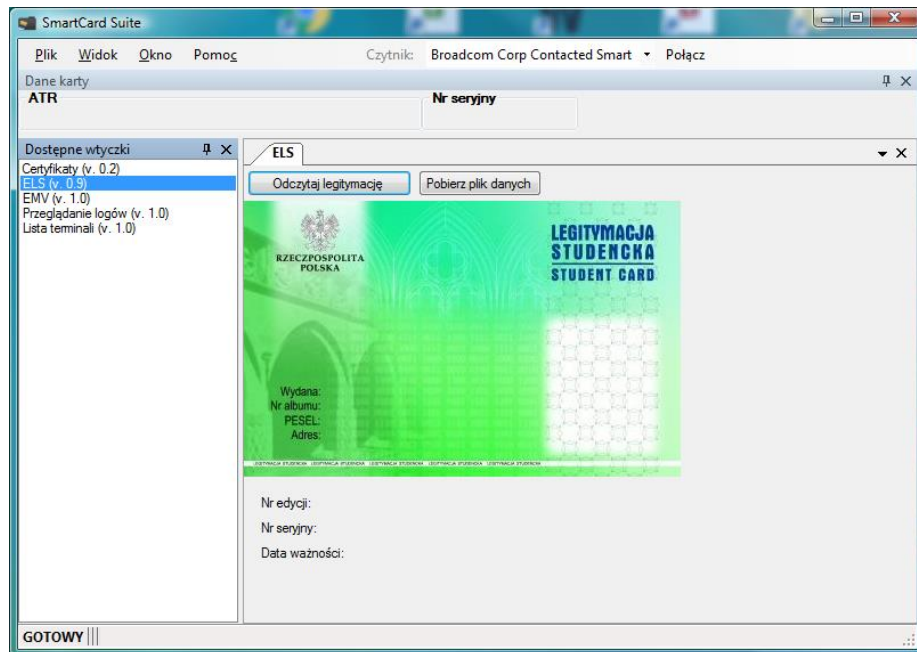
Caption: ([Update Colors](#))

UID & ManufInfo | ValueBlock | KeyA | KeyB | ACS

App Version: 1.0.0

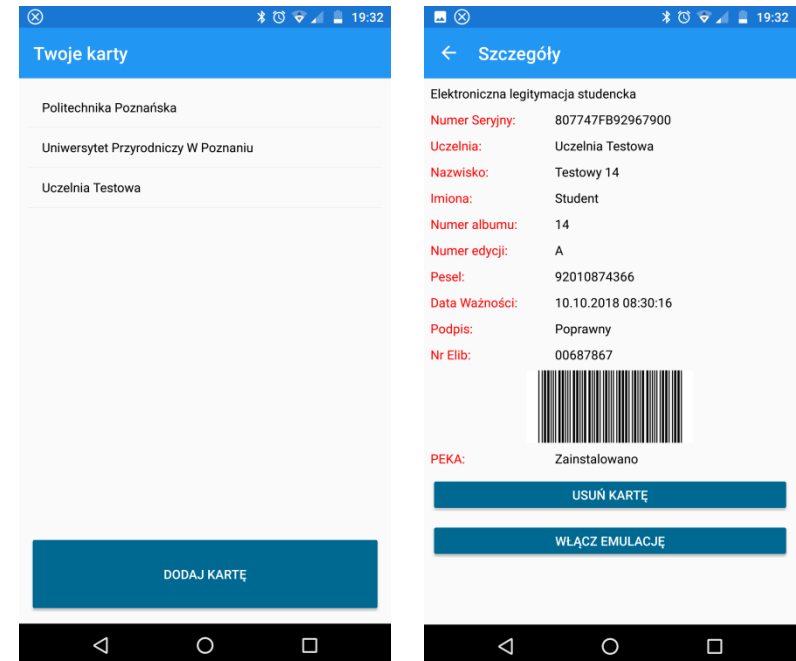
Inne oprogramowanie (android)

- SmartCardSuite
 - wtyczka „ELS”
- ELS ...
 - testy!
 - włączone do PPulse



Inne oprogramowanie

- PPulse
 - Funkcje ELS – praca dyplomowa
- PUT_els_nfs
 - Emulacja ELS w telefonie
 - praca dyplomowa



- marek.goslowski@put.poznan.pl
- +48 61 665 3680
- +48 694 949 750
- pl. Marii Skłodowskiej-Curie 5 (Wilda)
Budynek B1 (Rektorat), pok. 405
- <http://mcp.poznan.pl/>