

Laboratorium

Programowania Kart Elektronicznych

Elektroniczna Legitymacja Studencka

Marek Goślawski

Elektroniczna Legitymacja Studencka

- Przygotowanie do zajęć
 - sprawna legitymacja studencka
- Potrzebne wiadomości
 - język angielski w stopniu pozwalającym na czytanie dokumentacji technicznej
 - składnia poleceń i odpowiedzi APDU
 - zasady kodowania ASN.1
 - formaty: certyfikatu X.509, podpisu XAdES-BES
 - arytmetyka szesnastkowa

„Słowniczek”

- **ATR**
 - Answer To Reset (*MM, wykład 5*)
- **APDU**
 - Application Protocol Data Unit – struktura danych w protokole komunikacji między czytnikiem a kartą elektroniczną (*wiki*), (*MM, wykład 5*)
- **MF, DF, EF**
 - rodzaje plików – omówione dalej

„Słowniczek”

- **FCP**
 - File Control Parameter, 0x62,
 - np. nazwa, rozmiar, deskryptor, uprawnienia
- **FMD**
 - File Management Data, 0x64
- **FCI**
 - File Control Information = FCP + FMD, 0x6F

„Słowniczek”

- **ASN.1**

- Abstract Syntax Notation One, standard służący do opisu struktur przeznaczonych do reprezentacji, kodowania, transmisji i dekodowania danych *(wiki)*

- **X.509**

- standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu służących do budowania hierarchicznej struktury PKI

„Słowniczek”

- **XAdES**

- XML Advanced Electronic Signatures – format kwalifikowanego podpisu elektronicznego

- **XAdES-BES**

- Basic Electronic Signature – podstawowa forma rozwijająca podpis elektroniczny m.in. o czas lokalny, miejsce, role osoby składającej podpis, ścieżkę certyfikacji i inne ... *(wiki)*

Elektroniczna Legitymacja Studencka

- Oprogramowanie
 - Edsi EasyReader
 - przesyłanie poleceń APDU
 - HxD
 - edycja plików (kodowanie szesnastkowe)
 - ASN.1 Editor
 - dekodowanie struktury ASN.1
 - SmartCardSuite (zastępuje funkcje powyższych)
 - <http://sourceforge.net/projects/smartcardsuite/>
 - mile widziane wszelkie informacje o błędach, pomysły

Elektroniczna Legitymacja Studencka

- Zadania
 - odczytanie pliku EF.CERT
 - odczytanie pliku EF.ELS
 - interpretacja pliku EF.CERT – osoba przedłużająca
 - interpretacja pliku EF.ELS – numer układu
- Przesłanie na adres:
 - marek.goslowski@put.poznan.pl

Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

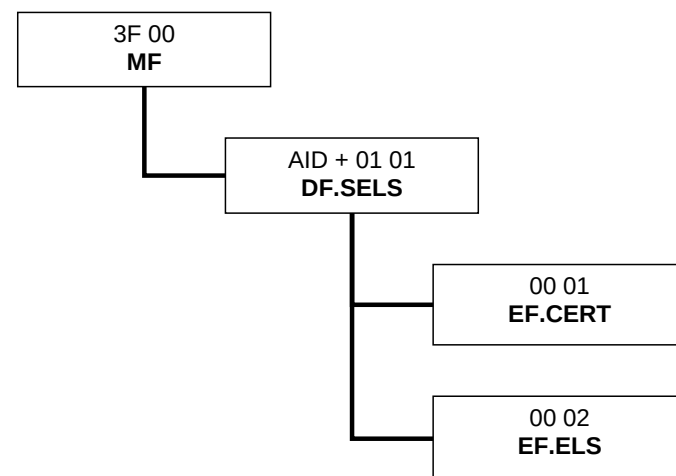
Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:

marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

- Struktura karty
 - rozporządzenie MNiSW z 27 września 2018 r. w sprawie studiów (D20181861.pdf)



Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

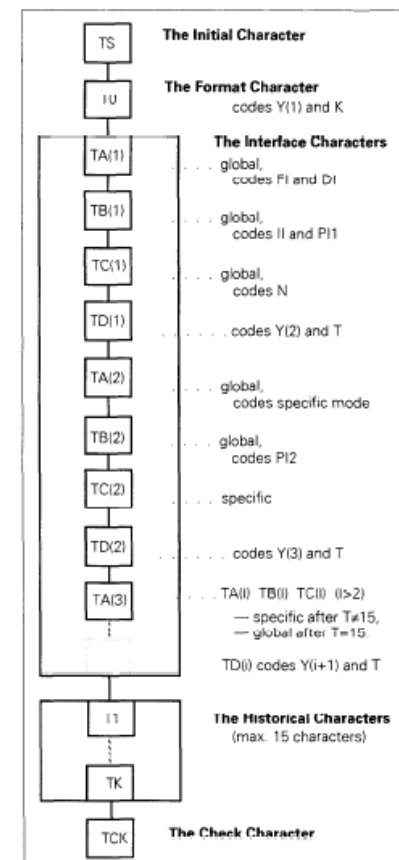
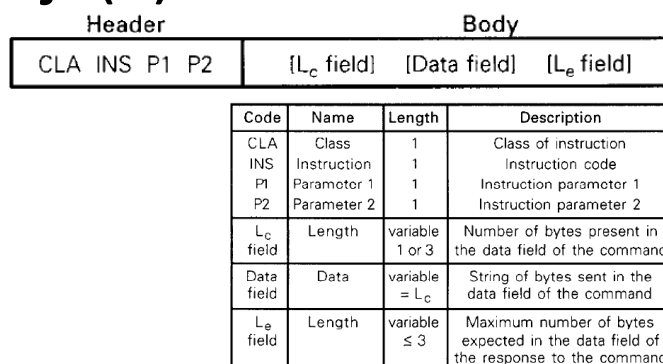
Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:

marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

- ATR karty (answer to reset)
 - ISO/IEC 7816-3
 - ISO/IEC 7816-4 (historical bytes)
 - protokół transmisji (?)
- APDU
 - ISO/IEC 7816-4



Zadanie 1: odczytanie pliku EF.CERT
 Zadanie 2: odczytanie pliku EF.ELS
 Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca
 Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:
marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

ATR: 3B FB 96 00 00 81 31 FE 45 00 31 C0 64 77 E9 10 00 01 90 00 EC

TS=3B (1=Z direct convention)

T0=FB

Interface Bytes	:	i	TAi	TBi	TCi	Tdi
		1	96	00	00	81
		2				31
		3	FE	45		

----- ISO 7816 - 3 -----

General parameters

Fi (TA1)	:	512 (max 5.0MHz)
Di (TA1)	:	32
Min etu	:	16 cycles (Fi/Di)
VPP param (TB1)	:	not used
N (TC1)	:	0 (Extra Guardtime)
Def. protocol (TDx)	:	T=1
Mode (TA2)	:	negotiable

T=1 parameters

IFSC (TA3,TA4,...)	:	254 (info field size)
CWI (TB3,TB4,...)	:	5 (char wait interval)
char wait time	:	43 etu, 4 ms (3.57MHz)
BWI (TB3,TB4,...)	:	4 (block wait interval)
block wait time	:	15371 etu, 1601 ms (3.57MHz)
err code (TC3,...)	:	lrc

6.4.2 ISO/IEC 7816-3

Figure 11: 1111 - występuje TA1, TB1, TC1, TD1, B (hex) bajtów historycznych

6.4.3.2 TA(i), TB(i), TC(i); 6.4.3.1 TD(i); 6.2 Parametr T

81(hex)=1000 0001, występuje tylko TD2, protokół T=1

6.5.1 opis poszczególnych bajtów

Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

Zadanie 4: interpretacja pliku EF.ELS – numer układu

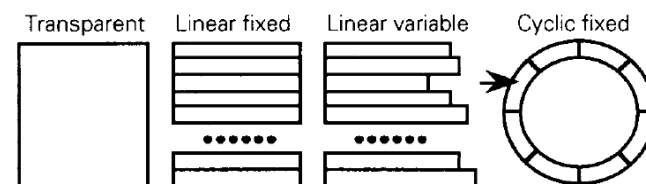
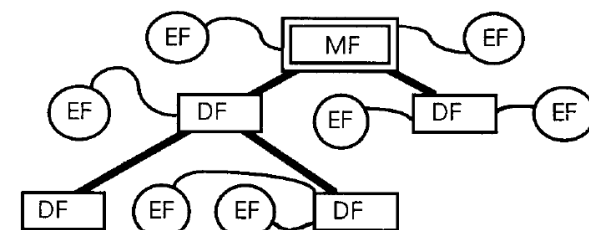
wysłać na adres:

marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

- Rodzaje plików

- MF (*master file*): katalog główny
- DF (*dedicated file*): katalog
- EF (*elementary file*): plik
 - przezroczysty (*transparent*)
 - liniowy (*linear*): stała, zmienna
 - cykliczny (*cyclic*): stały



Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:

marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

- Odczytanie pliku
 - wybór aplikacji/katalogu SELECT FILE
 - AID aplikacji ELS: D6 16 00 00 30 01 01
 - wybór pliku SELECT FILE
 - EF.CERT: 00 01
 - EF.ELS: 00 02
 - odczytanie części pliku READ BINARY/RECORD
 - odczytanie części pliku READ BINARY/RECORD

Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:

marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

- Odczytanie pliku EF.ELS

OberthurCS ID-One, Gemalto EMV / Gemalto

OberthurCS IAS

00A40000023F00

00A4040007D616000030010100

00A4040407D616000030010100

00A4000002000100

00A4020402000100

00B0000080

00B0000080

00B0008080 / 00B0002080 (bloki!)

00B0008080

00B0010080

00B0010080

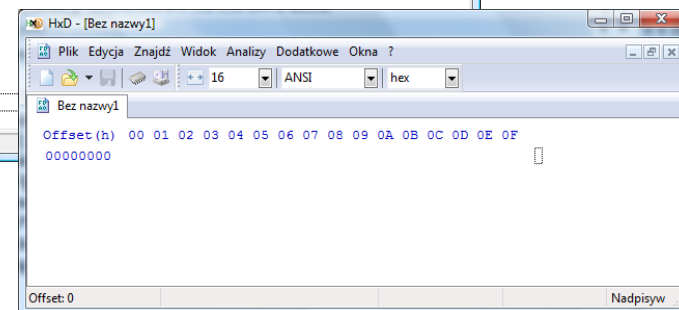
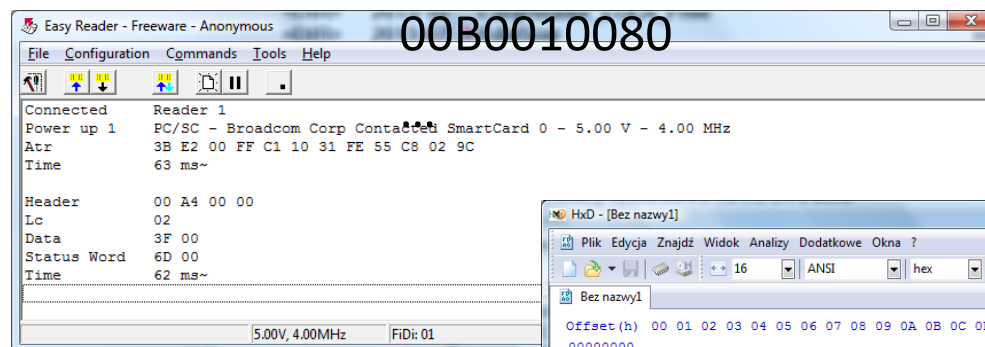
...

Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

Zadanie 4: interpretacja pliku EF.ELS – numer układu



Elektroniczna Legitymacja Studencka

- ASN.1 / TLV

– **Tag** (1 lub 2 bajty), **Length** (1, 2 lub 3 bajty), **Value**

→ 00 A4 04 04 07 **D6 16 00 00 30 01 01 00**

← **6F** 14 53 09 50 50 5F 45 4C 53 5F 01 00 84 07 D6 16 00 00 30 01 01

← **53** 09 50 50 5F 45 4C 53 5F 01 00 **84** 07 D6 16 00 00 30 01 01

- Tag '6F' – File control information (FCI template)
- Tag '53' – the value field of the data object consists of discretionary data not coded in TLV.
- Tag '84' – DF name

Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:

marek.goslowski@put.poznan.pl

Elektroniczna Legitymacja Studencka

- Interpretacja pliku EF.ELS

- ASN.1 (ISO/IEC 8825)

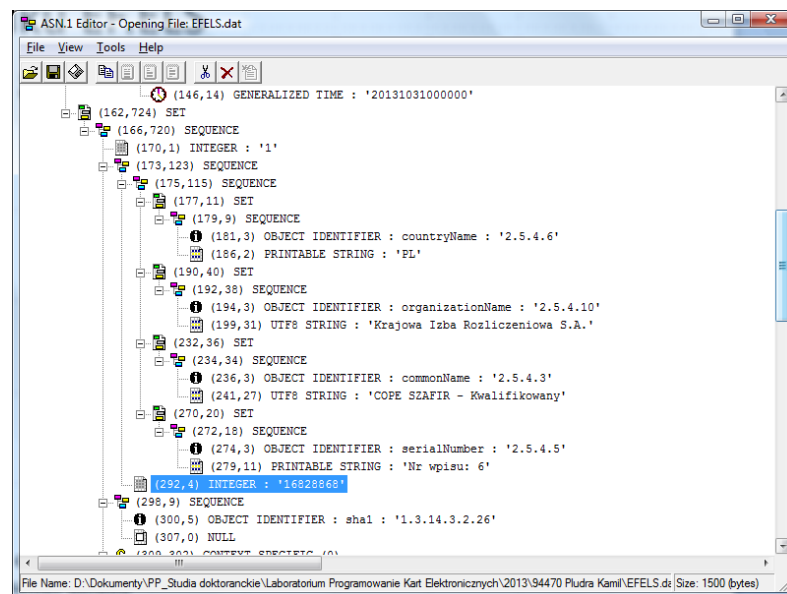
- podpisana struktura

- osoba podpisująca
na podstawie numeru
seryjnego certyfikatu

- sprawdzenie

- czy złożony w okresie ważności

- czy nie został unieważniony (np. listy CRL)



Zadanie 1: odczytanie pliku EF.CERT

Zadanie 2: odczytanie pliku EF.ELS

Zadanie 3: interpretacja pliku EF.CERT – osoba przedłużająca

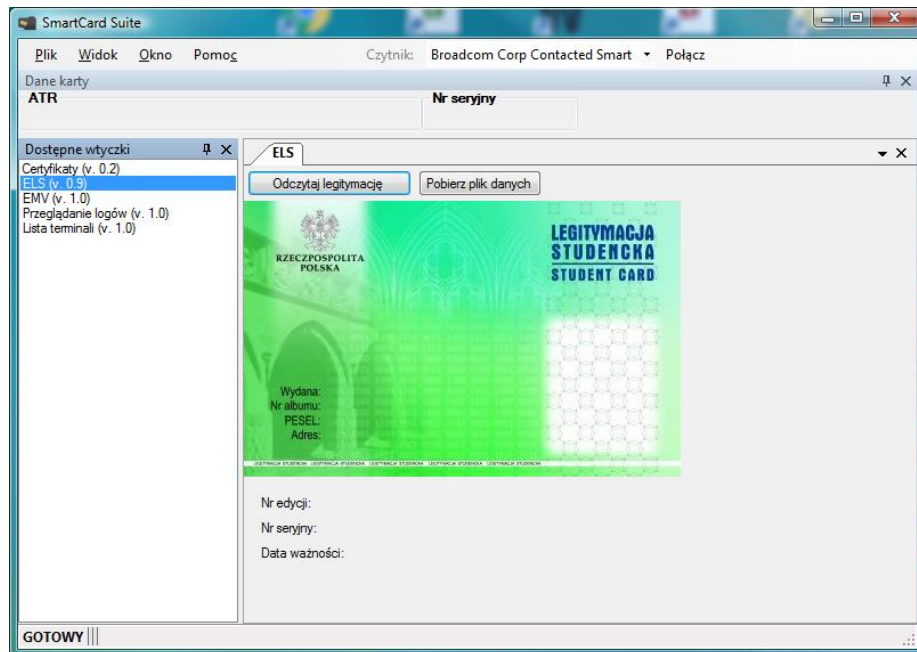
Zadanie 4: interpretacja pliku EF.ELS – numer układu

wysłać na adres:

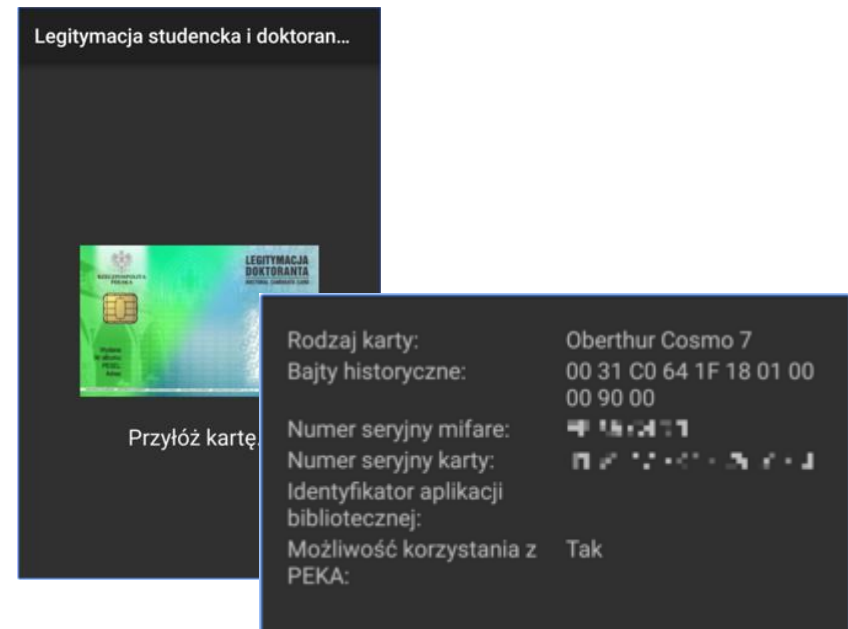
marek.goslowski@put.poznan.pl

Inne oprogramowanie

- SmartCardSuite
 - wtyczka „ELS”



- ELS ... (**Testy!**)
 - <https://play.google.com/store/apps/details?id=pl.poznan.put.els>



Inne oprogramowanie

- PPulse
 - Funkcje ELS – 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/>