

# Laboratorium

# Programowania Kart Elektronicznych

Karta SIM

Marek Goławski

# Karta SIM

- Przygotowanie do zajęć
  - karta SIM
  - dokumentacja ETSI TS 100 977
- Potrzebne wiadomości
  - język angielski w stopniu pozwalającym na czytanie dokumentacji technicznej
  - składnia poleceń i odpowiedzi APDU
  - podstawowa znajomość technologii GSM

# Karta SIM

- Oprogramowanie
  - Edsi EasyReader
    - przesyłanie poleceń APDU
  - Oprogramowanie dedykowane do kart SIM
  - SmartCardSuite (zastępuje funkcje powyższych)
    - <http://sourceforge.net/projects/smartcardsuite/>
    - mile widziane wszelkie informacje o błędach, pomysły

# „Słowniczek”

- **GSM**

- Global System for Mobile Communications, (pierwotnie Groupe Spécial Mobile), najpopularniejszy standard telefonii komórkowej

- **SIM**

- Subscriber Identity Module, moduł identyfikacji abonenta, najczęściej karta elektroniczna o zmniejszonych rozmiarach (miniSIM, mikroSIM, nanoSIM)

# „Słowniczek”

- **IMSI**

- International Mobile Subscriber Identity, unikatowy numer przypisany do każdej karty SIM w sieci GSM lub UMTS, jednoznacznie ją identyfikujący

- składa się z:

- kodu kraju MCC, Mobile Country Code (dla PL=260),
- kodu sieci MNC, Mobile Network Code (T-Mobile=02),
- numeru identyfikacyjnego abonenta ruchomego MSIN, Mobile Subscriber Identification Number

# „Słowniczek”

- **MSISDN**
  - Mobile Station International Subscriber Directory Number, numer abonenta sieci komórkowej, numer telefonu
- **ADN**
  - Abbreviated dialing numbers, Skrócone numery wybierania, książka telefoniczna

# Karta SIM

- Zadania
  - odczytanie numeru IMSI
  - odczytanie numeru telefonu z karty SIM
  - odczytanie numerów telefonów z książki tel.
  - zapisanie swojego kontaktu na karcie SIM
    - nazwisko, indeks, numer, 16 (10hex) komórka pamięci
- przesyłanie (logi z EasyReader) na adres:
  - [marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

Zadanie 1: odczytanie numeru IMSI

Zadanie 2: odczytanie numeru telefonu z karty SIM

Zadanie 3: odczytanie numerów telefonów z książki tel.

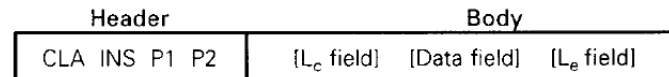
Zadanie 4: zapisanie swojego kontaktu na karcie SIM

wysłać na adres:

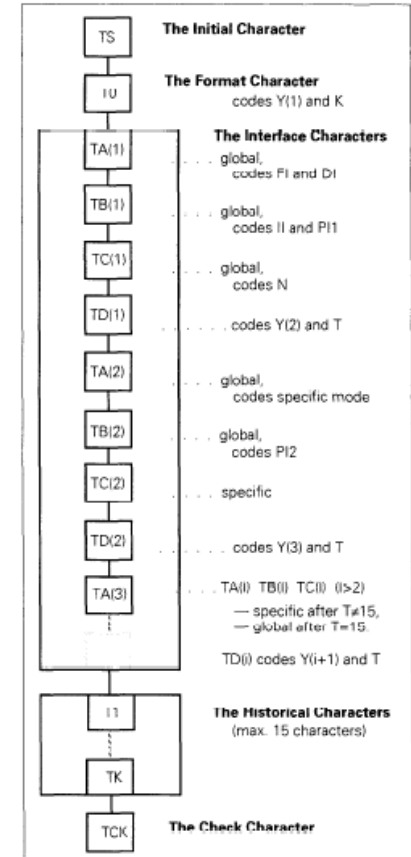
[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

# Karta SIM

- ATR karty (answer to reset)
  - protokół transmisji (?)
- APDU
  - CLA (?)
  - ETSI TS 100 977 rozdział 9.1



Code	Name	Length	Description
CLA	Class	1	Class of instruction
INS	Instruction	1	Instruction code
P1	Parameter 1	1	Instruction parameter 1
P2	Parameter 2	1	Instruction parameter 2
L <sub>c</sub> field	Length	variable 1 or 3	Number of bytes present in the data field of the command
Data field	Data	variable = L <sub>c</sub>	String of bytes sent in the data field of the command
L <sub>e</sub> field	Length	variable ≤ 3	Maximum number of bytes expected in the data field of the response to the command



- Zadanie 1: odczytanie numeru IMSI
- Zadanie 2: odczytanie numeru telefonu z karty SIM
- Zadanie 3: odczytanie numerów telefonów z książki tel.
- Zadanie 4: zapisanie swojego kontaktu na karcie SIM

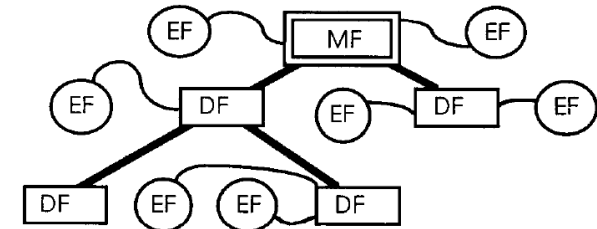
wysłać na adres:  
[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)



# Karta SIM

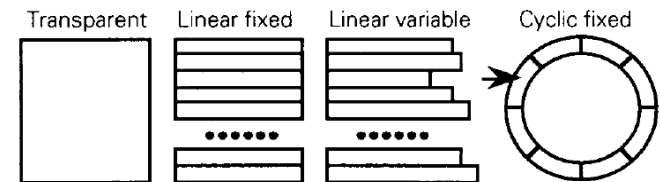
- Rodzaje plików

- MF (*master file*): katalog główny
- DF (*dedicated file*): katalog
- EF (*elementary file*): plik
  - przezroczysty / liniowy / cykliczny



- Struktura plików

- ETSI TS 100 977, rozdział 10



Zadanie 1: odczytanie numeru IMSI

Zadanie 2: odczytanie numeru telefonu z karty SIM

Zadanie 3: odczytanie numerów telefonów z książki tel.

Zadanie 4: zapisanie swojego kontaktu na karcie SIM

wysłać na adres:

[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

# Karta SIM

- Odczytanie / zapis pliku
  - wybór aplikacji/katalogu SELECT FILE
  - wybór pliku SELECT FILE
  - odczytanie części pliku READ BINARY/RECORD
  - zapis części pliku UPDATE BINARY/RECORD
  - odczytanie odpowiedzi GET RESPONSE
- ETSI TS 100 977, rozdział 9.2

Zadanie 1: odczytanie numeru IMSI

Zadanie 2: odczytanie numeru telefonu z karty SIM

Zadanie 3: odczytanie numerów telefonów z książki tel.

Zadanie 4: zapisanie swojego kontaktu na karcie SIM

wysłać na adres:

[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

# Karta SIM

- Nazwy plików
  - $DF_{\text{GSM}}/EF_{\text{IMSI}}$  (IMSI)
  - $DF_{\text{TELECOM}}/EF_{\text{MSISDN}}$
  - $DF_{\text{TELECOM}}/EF_{\text{ADN}}$

Zadanie 1: odczytanie numeru IMSI

Zadanie 2: odczytanie numeru telefonu z karty SIM

Zadanie 3: odczytanie numerów telefonów z książki tel.

Zadanie 4: zapisanie swojego kontaktu na karcie SIM

wysłać na adres:

[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

# Karta SIM

- Odczytywanie informacji o pliku
  - GET RESPONSE w odpowiedzi na SELECT FILE (EF)

RECV	00 00	<i>RFU</i>
	00 09	<i>File size</i>
	6F 07	<i>File ID</i>
	04	<i>Type of file (see 9.3) ... '04' EF</i>
	00	
	1A FF 1F	<i>Access conditions (see 9.3)</i>
	01	<i>File status (see 9.3)</i>
	02	<i>Length of the following data</i>
	00	<i>Structure of EF (see 9.3)</i>
	<b>00</b>	<b><i>Length of a record</i></b>

Zadanie 1: odczytanie numeru IMSI

Zadanie 2: odczytanie numeru telefonu z karty SIM

Zadanie 3: odczytanie numerów telefonów z książki tel.

Zadanie 4: zapisanie swojego kontaktu na karcie SIM

wysłać na adres:

[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

# Karta SIM

- Kodowanie numerów telefonów

- rozdział 10.5.1

- tabela 12

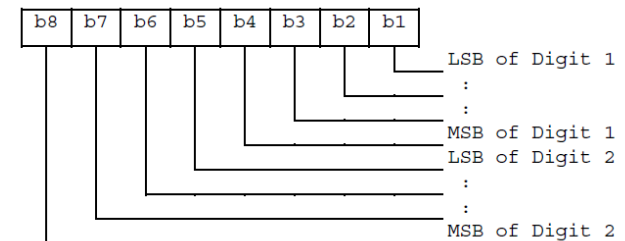
- wartość X (?)

- GET RESPONSE w odpowiedzi na SELECT FILE

00 00 00 54 6F 40 04 00 11 FF FF 01 02 01 **1C**

X+14 bytes = 1C → X = ?

Byte X+3



Zadanie 1: odczytanie numeru IMSI

Zadanie 2: odczytanie numeru telefonu z karty SIM

Zadanie 3: odczytanie numerów telefonów z książki tel.

Zadanie 4: zapisanie swojego kontaktu na karcie SIM

wysłać na adres:

[marek.goslowski@put.poznan.pl](mailto:marek.goslowski@put.poznan.pl)

- [marek.goslowski@put.poznan.pl](mailto: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/>