Karty mikroprocesorowe

Notatki z wykładu

Struktura karty mikroprocesorowej

Są to karty zabezpieczone lepiej niż karty magnetyczne. Mają przy tym takie same wymiary jak karty magentyczne. Posiadają jednak dodatkowy styk, znadujący się na awersie karty. Musi się on składać z:

- Panelu z napięciem odniesienia (GND)
- Styk informacyjny input/output działający w trybie simplex
- Panel doprowadzający zewnętrze programowania (V_{PP}), które dostarcza energię do karty podczas zapisu do niej

Nawiązanie połączenia z kartą

Karta po włożeniu do interfejsu stykowego otrzymuje sygnal RESET. Odpowiada na niego 32-znakową sekwencją ATR (eng. answer to reset), która przenosi dane o:

- Rodzaju karty
- Sposobie kodowania bitów
- Protokole komunikacji (który jest niezbędny ze względu na działanie w trybie simplex)

Struktura wiadomości ATR

Znak inicjalizacji TS	Długość trwania impulsu znaku inicjalizacji określa długość trwania bitu nadawanego przez kartę. Owa długość nazywana jest ETU (elementary time unit).
Znak formatujący	
Znaki z danymi	ATR może zawierać w sobie *n*-ogniw zawierających dane.
Znaki historyczne	
Suma kontrolna	

Znak formatu

Znak formatu to 5-bajtowa struktura zawierająca informacje o:

- Liczbie znaków historycznych. Owa informacja zapisana jest w formie mapy bitowej (rejestru flat bitowych) określającej jaki znak występuje a jaki nie występuje.
- Liczbie znaków w następnym ogniwie z danymi. Przy czym ciąg samych ‘0’ oznacza, że następne ogniwo nie istnieje, a obecny znak jest ostatni.
- Częstotliwości sygnału zegarowego
- Napięciach, mocach i prądach niezbędnych do poprawnego programowania karty
- Numerze protokołu, w którym porozumiewa się karta. Najczęściej dostępnymi protokołami są T_0 lub T_1.

Application PDU (APDU)

Protokół określający sposób simplexowej komunikacji z kartą mikroprocesorową. Zgodnie z nim w ramach takiej komunikacji karta może tylko odpowiadać a interfejs stykowy tylko nadaje. Komunikacja odbywa się w formie komenda-odpowiedź.

Command PDU
Jednostka danych przenosząca ze sobą komendę dla karty mikroprocesorowej. Wysyłana przez interfejs stykowy.

Klasa karty	0xA0 – karta GSIM 0x80 – karty pamięci 0x00 – karty bankowe (standardu ISO 7816)
ID Instrukcji	1-bajtowe
Parametr 1	1-bajtowy parametr
Parametr 2	1-bajtowy parametr
Długość pola danych	
Dane	
Spodziewana długość odpowiedzi	

https://cardwerk.com/smart-card-standard-iso7816-4-section-6-basic-interindustry-commands/

SELECT FILE
Komenda wybierająca plik. Id komendy to 0xA4. Danymi jest 2-bajtowy adres pliku.

CLA	INS	P1	P2	Lc	Data
0xA0	0xA4	0x00	0x00	0x02	0x7F 0x10

- CLA = 0xA0 – karty SIM
- INS = 0xA4 – SELECT
- Lc = 0x02 – długość adresu
- Data = adres złożony z 2 znaków: 7F10

https://cardwerk.com/smart-card-standard-iso7816-4-section-6-basic-interindustry-commands/#chap6_11_1

GET RESPONSE
Komenda pobierająca z karty odpowiedź na ostatnią komendę.ID komendy to 0xC0.

CLA	INS	P1	P2	Le	
0xA0	0xC0	0x00	0x00	0x16	

- CLA = 0xA0 – karty SIM
- INS = 0xC0 – GET RESPONSE
- Le = 0x16 – długość spodziewanej odpowiedzi

READ RECORD
Komenda odczytująca rekord z aktualnie wybranego EF. Id komendy to: 0xB2.

CLA	INS	P1	P2	Le	
0xA0	0xB2	0x03	0x04	0xB0	

- CLA = 0xA0 – karty SIM
- INS = 0xB2 – READ RECORD
- P1 = 0x03 rekord 3
- P2 = 0x04 specyfikacja odczytu: 4 oznacza tylko rekord 3
- Le = 0xB0 – długość spodziewanej odpowiedzi

https://cardwerk.com/smart-card-standard-iso7816-4-section-6-basic-interindustry-commands/#chap6_5_1

Response PDU

Jednostka danych przenoszące ze sobą odpowiedź karty na komendę. Wysyłana przez kartę.

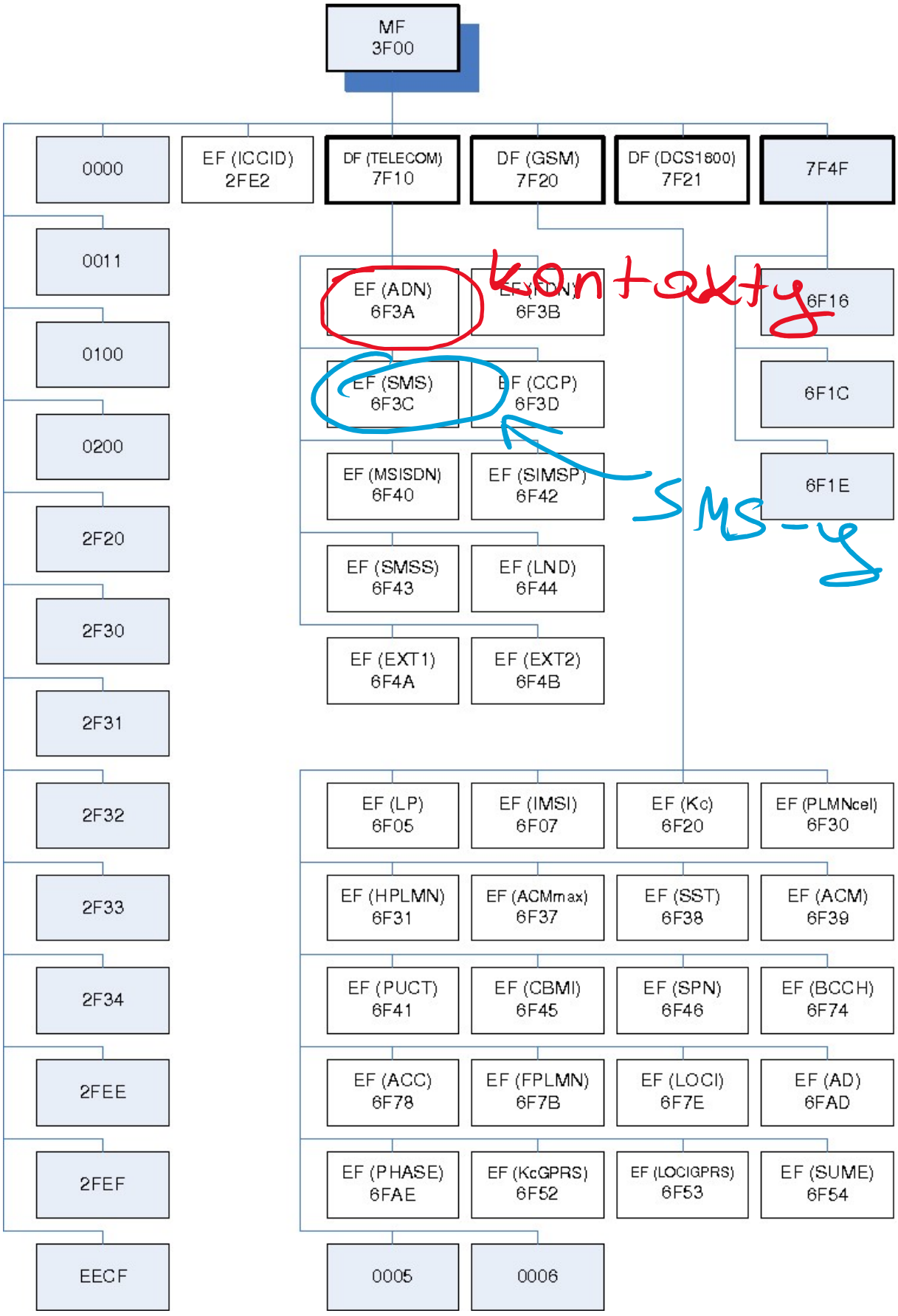
Dane odpowiedzi	
Słowo statusowe	Informacja 2-bajtowa informująca np. o wystąpieniu błędu.

Słowa statusowe

Zbiory na karcie

- **Katalog główny** – inaczej nazwyany jako master file (MF). Odpowiednik folderu root.
- **Katalog karty** – inaczej nazywany jako dedicated file (DF). Odpowiedniki folderów.
- **Zbiór** – inaczej nazywany jako elementary file (EF). Odpowiedniki plików. Dzielą się one na
  - *Bez struktury* – zawierające wyłącznie dane binarne
  - *O Stałych rekordach* – składające się z wierszy stałej długości
  - *O różnych rekordach* – składające się z wierszy różnej długości
  - *Cykliczne* – których wiersze tworzą cykl

Każdy ze zbiorów na karcie ma ponadto przypisany 2-bajtowy adres, który zapisywany jest w postaci heksadecymalnej.


MF
3F00
0000
EF (ICCID)
2FE2
DF (TELECOM)
7F10
DF (GSM)
7F20
DF (DCS1800)
7F21
7F4F
0011
0100
0200
2F20
2F30
2F31
2F32
2F33
2F34
2FEE
2FEF
EECF
EF (ADN)
6F3A
EF (EXT1)
6F3B
EF (SMS)
6F3C
EF (CCP)
6F3D
EF (MSISDN)
6F40
EF (SIMSP)
6F42
EF (SMSS)
6F43
EF (LND)
6F44
EF (EXT1)
6F4A
EF (EXT2)
6F4B
6F16
6F1C
6F1E
kontakty
SMS-y
EF (LP)
6F05
EF (IMSI)
6F07
EF (Kc)
6F20
EF (PLMNcel)
6F30
EF (HPLMN)
6F31
EF (ACMmax)
6F37
EF (SST)
6F38
EF (ACM)
6F39
EF (PUCT)
6F41
EF (CBMI)
6F45
EF (SPN)
6F46
EF (BCCH)
6F74
EF (ACC)
6F78
EF (FPLMN)
6F7B
EF (LOCI)
6F7E
EF (AD)
6FAD
EF (PHASE)
6FAE
EF (KcGPRS)
6F52
EF (LOCIGPRS)
6F53
EF (SUME)
6F54
0005
0006