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 (VPP­), 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 *T0* lub *T1*.

# 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.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

<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.

Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

### READ RECORD

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

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

<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

Możemy wyróżnić następujące słowa statusowe:

* 0x90 0x00 – komenda wykonała się w pełni poprawnie
* 0x61 0x\*\* - komenda wykonałą się poprawnie, ale nieodczytane zostało \*\* bajtów
* 0x69 0x\*\* - komenda niedozwolona. Kod \*\* koduje przyczynę.
* 0x6A 0x\*\* - parametr 1 lub/i pareametr 2 są błędne

# 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.



