Karty inteligentne - programowanie i zastosowania

Piotr Nazimek

Instytut Informatyki Politechniki Warszawskiej
Warszawa 2005

Plan seminarium

- karty elektroniczne - wprowadzenie
- komunikacja
  - protokoły
  - czytniki
  - interfejsy
- systemy operacyjne kart
  - na przykładzie MPCOS
- przykład: elektroniczna legitymacja studenta

Karty elektroniczne

- kawałek plastiku z wbudowanym układem elektronicznym
- często, choć niepoprawnie nazywane ~~kartami czipowymi~~
- komunikacja oraz zasilanie układu realizowane jest poprzez fizyczne połączenie lub drogą radiową
- różne klasyfikacje kart
  - budowę
  - możliwości
  - zastosowania
  - interfejsy komunikacyjne

Karty pamięciowe

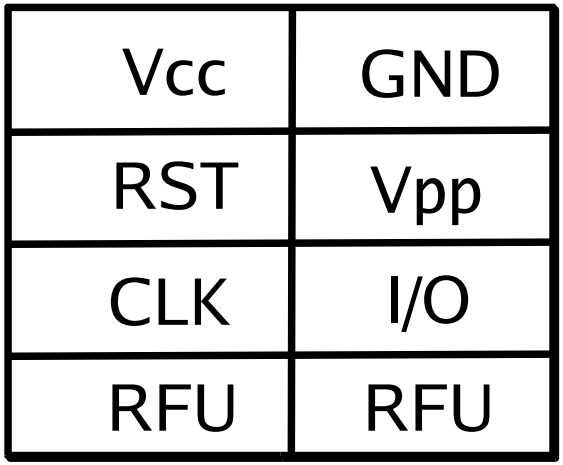
- karty elektroniczne posiadające pewien obszar pamięci służący do przechowywania danych
- z lub bez ochrony pamięci
- zapis/odczyt – odnosi się do struktury fizycznej karty
- sposób komunikacji, zapisu/odczytu do/z pamięci nie jest ustandaryzowany
- przykłady:
  - karta telefoniczna
  - karta zdrowia

Karty procesorowe

- wyposażone w system operacyjny
- inne określenia:
  - karta mikroprocesorowa
  - karta inteligentna
  - ang. *smart card*
- producenci: Gemplus, Setec, Axalto (Schlumberger), G&D, ...
- przykłady
  - karta SIM
  - karta VITAY

Karty stykowe i bezstykowe

- karty stykowe



- karty bezstykowe
  - zasilanie i komunikacja drogą radiową
  - trzy rodzaje kart (w zależności od zasięgu)

Karty hybrydowe i dualne

- podział umowny
- interfejs stykowy i bezstykowy – karta *dualna*
- układ elektroniczny + pasek magnetyczny – karta *hybrydowa*

Karty „natywne” i „programowalne”

- karty „natywne”
  - posiadają system operacyjny o określonym zestawie rozkazów
  - przechowywanie i zarządzanie dostępem do danych
  - specjalizacja
- karty „programowalne”
  - możliwość stworzenia aplikacji jako „kawałka systemu operacyjnego”
  - dodatkowo możliwość implementacji logiki aplikacji
  - Java Card, .NET Card, MULTOS

Formaty kart

- najbardziej popularne
  - ID 1 – karta płatnicza
  - ID 000 – karta SIM
- ID 00 – rozmiar pomiędzy kartą SIM a płatniczą
- określone w ISO/IEC 7810

Zastosowania

- jako „bezpieczny nośnik informacji”
- systemy płatnicze (EMV, elektroniczne portmonetki)
- systemy lojalnościowe
- podpis elektroniczny
- systemy dostępu
- systemy transportu publicznego (elektroniczny bilet)
- telefonia komórkowa (karta SIM)

Komunikacja

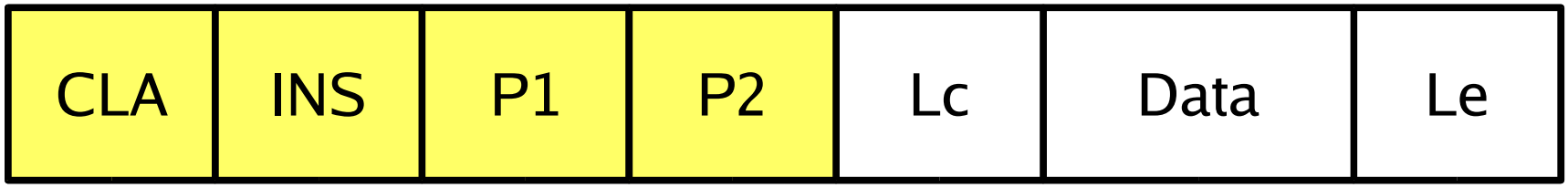
- protokół wyzwanie-odpowiedź
- protokoły
  - T=0 – prosty, najczęściej używany (znakowy)
  - T=1 – komunikat „zanurzony” w pakiecie (blokowy)
  - T=USB – dla kart USB
- komunikat PTS (ang. ***P****rotocol* ***T****ype* ***S****election*)

ATR

- ang. *Answer To Reset*
- po dostarczeniu napięcia do karty
- określa możliwości karty (protokół komunikacyjny, szybkość transmisji)
- pozwala zidentyfikować rodzaj karty
- zawiera dodatkowe informacje producenta

APDU

- ang. ***A**pplication **P**rotocol **D**ata **U**nit*
- rozkaz przesyłany do karty



- ISO 7816-4 – określono standardowe komendy

RAPDU

- ang. ***R**esponse **A**pplication **P**rotocol **D**ata **U**nit*
- odpowiedź karty

- ISO 7816-4 - określono standardowe bajty statusu

Czytniki kart

- interfejs pomiędzy kartą a systemem zewnętrznym
- RS232, USB, PCIMCIA, ISA, wbudowane
- różne API
  - CT-API (głównie C)
  - PC/SC (C, C++, Java, Perl, Python, ...)
  - OCF (Java)
  - inne
- podstawowe komendy
  - inicjalizuj
  - wyślij/odbierz
  - zakończ sesję

CT-API

- ang. ***C****ardT****e****rminal - **A****pplication **P****rogramming **I****nterface*
- jedynie trzy komendy
  - najczęściej interfejs w języku C
- zalety
  - prostota
- wady
  - konsolidacja bibliotek zależnych od urządzeń
  - aplikacja zależna od określonego urządzenia

PC/SC

- ang. ***P**ersonal **C**omputer/**S**mart **C**ard*
- zarządzanie czytnikami i kartami w systemie
  - uniwersalne API niezależne od czytnika
  - zarządzanie dostępem (transakcje)
- czytniki zgodne z PC/SC
- standardowy sposób korzystania z „zasobów” w systemie MS Windows
- implementacje dla innych systemów operacyjnych
- http://www.pcscworkgroup.com/

OCF (Open Card Framework)

- biblioteka stworzona w języku Java
- podejście obiektowe
- pozwala na stworzenie aplikacji (apletu) klienta korzystającego z czytników i kart działających w systemie operacyjnym
- dzięki implementacji w Java – jest przenośna (jeśli stworzono „natywne” biblioteki do komunikacji...)
- pozwala na wszechstronną konfiguracje i użycie tego samego kodu dla np. rzeczywistej karty i symulatora
- http://www.opencard.org/

Inne interfejsy

- implementacje interfejsu PC/SC w innych językach
  - Perl, Python, Java
- OpenCT
  - integracja czytników PC/SC, CT-API i OpenCT
- telefony komórkowe – SATSA
  - ang. *Security and Trust Services*
- inne urządzenia
- API dla systemów operacyjnych kart

Systemy operacyjne kart

- COS, ang. ***C****ard* ***O****perating* ***S****ystem*
- specjalizacja dla określonego zastosowania (karty „natywne”)
  - kryptograficzne
  - lojalnościowe
  - płatnicze itp.
- istotne różnice pomiędzy systemami
- systemy z maszynami wirtualnymi
  - Java Card, .NET Card

ISO 7816-4

- seria norm dotyczących kart inteligentnych
- opisuje komendy „wspólne” dla kart
  - operujące na plikach: SELECT FILE, CREATE FILE, READ BINARY, WRITE BINARY, UPDATE BINARY ...
  - GET CHALLENGE
  - GET RESPONSE
- większość kart posiada zaimplementowane komendy z ISO 7816-4 + dodatkowe (zależne od producenta)

Obsługa plików

- hierarchiczny system plików
- MF (ang. ***M**aster **F**ile*, FID '3F00')
  - DF (ang. ***D**edicated **F**ile*)
    - EF (ang. ***E**lementary **F**ile*)
  - DF
    - EF
    - EF
  - EF
- różne typy plików EF
  - transparentne, rekordowe, cykliczne, przechowujące kody PIN...
- prawa dostępu do plików

Zabezpieczenia

- uwierzytelnienie przed wykonaniem określonych operacji
  - wyzwanie-odpowiedź
  - kod PIN
- zabezpieczona komunikacja (ang. *secure messaging*)
- moduły SAM (ang. ***S**ecure **A**ccess **M**odule*)
- zabezpieczenia sprzętowo-implementacyjne
  - anty DPA, liczniki prób, atomowość transakcji

MPCOS EMV R5 2000

- ***M**ulti-application **P**ayment **C**hip **O**perating **S**ystem*
- ***E**uropay-**M**asterCard-**V**isa*
- ***R**evision 5*
- *2000 = 2kB*
- karta firmy Gemplus
- podstawowe zastosowania
  - wieloaplikacyjna elektroniczna portmonetka
  - karta płatnicza EMV

Charakterystyka MPCOS

- zgodna z ISO 7816-4
- komendy dla elektronicznej portmonetki
  - READ BALANCE
  - CREDIT
  - DEBIT itp.
  - „podpisywanie” transakcji
- obsługa PIN
- operacje kryptograficzne oparte o algorytm 3DES z klucz 16-sto bajtowy

Charakterystyka MPCOS

- prawa dostępu do plików
  - użycie pliku zależne od uwierzytelnienia określonym kluczem
  - „zamrażanie” praw
- założonych plików... nie można usunąć
  - utrudnienie w testowaniu np. personalizacji z kartą
  - alternatywa: karta GPK (MPCOS + kryptografia asymetryczna)
    - posiada komendę „developerską” ERASE CARD

Charakterystyka MPCOS

- możliwość identyfikacji aplikacji bez użycia FID
  - AID (ang. ***A**pplication **ID***) – unikalny identyfikator DF, w którym znajdują się dane aplikacji
    - do 16 bajtów
- istnieje moduł SAM odzwierciedlający operacje kryptograficzne dla MPCOS
  - dywersyfikacja kluczy kryptograficznych
    - algorytm wyprowadzenia klucza *per karta* na podstawie unikalnego numeru karty i klucza matki
- inne wielkości pamięci: 8kB, 32kB

Przykład komunikacji

3B 24 00 80 72 94 43

00 84 00 00 08

32 89 FA D8 10 67 A1 C7 90 00

itd...

Podsumowanie

- rozwój aplikacji kartowej – odzwierciedla cykl życia karty
  - personalizacja
    - wprowadzenie kluczy i danych
  - karta u użytkownika
    - użytek codzienny
    - operacje administratora
  - zakończenie życia karty

Co dalej?

- SIM
  - http://www.etsi.org/
- EMV
  - http://www.emvco.com/
- OpenSC i OpenCT
  - http://www.opensc.org
- Java Card (dokumentacja + API + symulator)
  - http://java.sun.com/products/javacard/
- grupa dyskusyjna (FAQ)
  - news:alt.technology.smartcards

Co dalej?

- PKCS #11 i #15
  - http://www.rsasecurity.com/
- GlobalPlatform
  - http://www.globalplatform.org/
- Linux
  - http://www.linuxnet.com
- inne dokumenty
  - http://www.google.com
  - http://clusty.com/

Elektroniczna legitymacja studenta

- projekt wprowadzenia dokumentu
  - zastąpienie książeczkowej legitymacji
  - podwyższenie bezpieczeństwa
  - prestiż
- integracja z istniejącymi systemami na uczelniach oraz lokalnymi usługami
- aspekt biznesowy (?)
  - karty są popularne i „pożądane”

Zawartość

- dane jednoznacznie identyfikujące studenta
  - dostępne dla zainteresowanych podmiotów
  - modyfikowalne wyłącznie przez uprawnione instytucje
- dane zabezpieczone podpisem elektronicznym (kwalifikowanym)
  - „ustawowe” upowszechnianie podpisu
- dane o ustalonej strukturze, składni i lokalizacji w pamięci (fizycznej, logicznej) karty

MIFARE ®

- bezstykowa karta pamięciowa z ochroną pamięci
- do wykorzystania 768 bajtów (w karcie 1kB)
  - podzielone na 16 sektorów
  - sektor składa się z czterech 16-sto bajtowych bloków
  - można określić zasady dostępu do każdego z bloków
- jest to standard przemysłowy firmy Philips
  - wiele firm ma w ofercie tą kartę
- zastosowania:
  - systemy dostępu
  - bilet elektroniczny

MIFARE ®

- niska uniwersalność zapisu
  - upychanie danych w 768 bajtach
  - „uproszczony” certyfikat (?)
  - nielogiczny zapis i odczyt
    - to jest karta o innym przeznaczeniu
- stałe przywiązanie do „firmowej” technologii
- uniemożliwienie integracji z lokalnymi systemami dostępu, „kartami miejskimi”
- niska cena

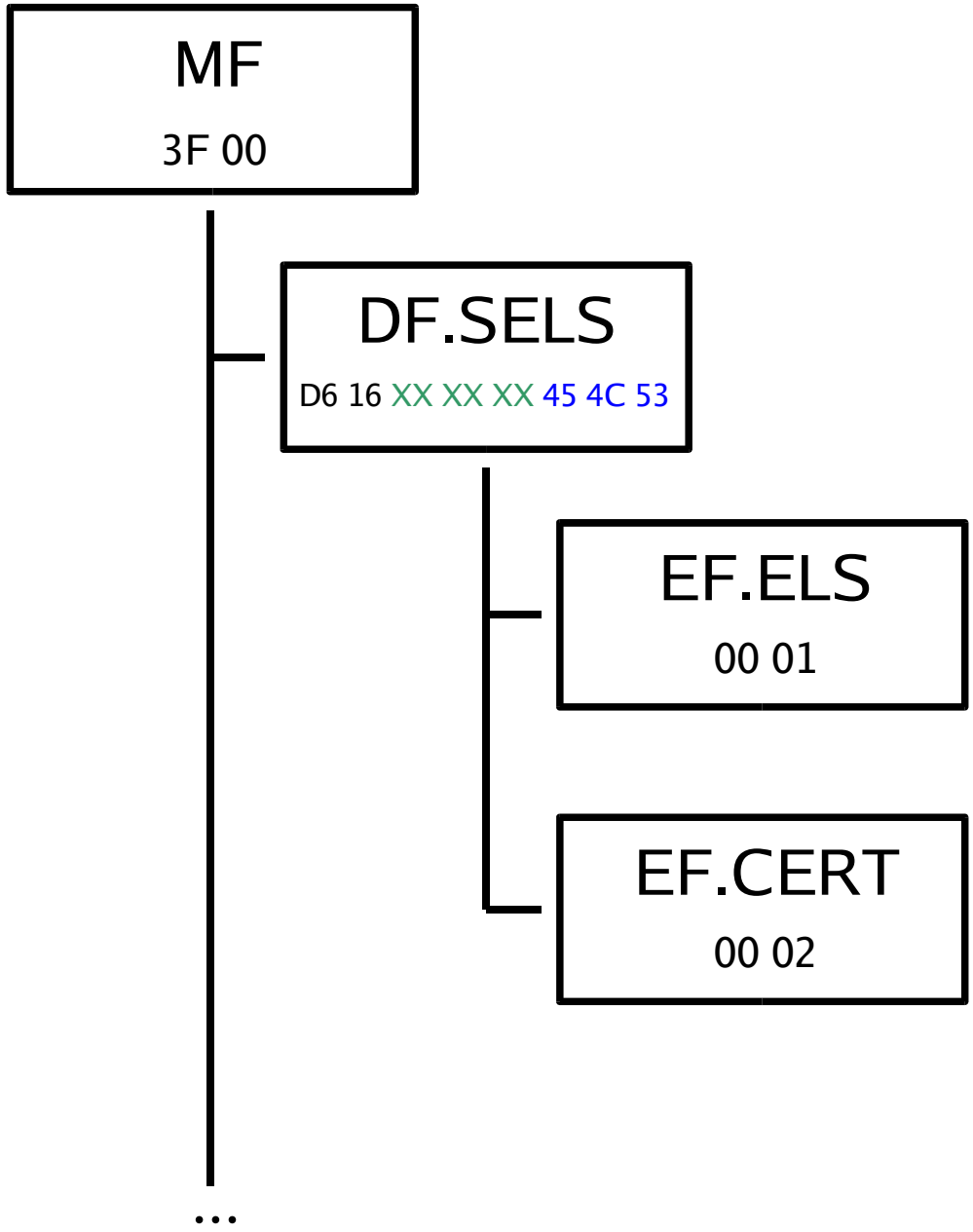
Aplikacja w karcie stykowej

- zarejestrowany identyfikator aplikacji (AID)
- zarejestrowany identyfikator obiektu (OID)
- uniwersalny opis danych (logiczny) z użyciem ASN.1
- możliwość realizacji na praktycznie wszystkich kartach
- możliwość rozwoju aplikacji bez wymiany technologii
- wieloaplikacyjność legitymacji

Aplikacja w karcie stykowej

```
SELSInfo ::= SEQUENCE
{
    numerSeryjnyUkladu      PrintableString (SIZE (8..16)),
    nazwaUczelni            UTF8String (SIZE (1..128)),
    nazwiskoStudenta        SEQUENCE OF UTF8String (SIZE (1..28)),
    imionaStudenta          SEQUENCE OF UTF8String (SIZE (1..24)),
    numerAlbumu             PrintableString (SIZE (1..16)),
    numerEdycji             PrintableString (SIZE (1)),
    numerPesel              PrintableString (SIZE (11)),
    dataWaznosci            GeneralizedTime
}
```

Aplikacja „legitymacja”



Cykl życia

- personalizacja
- wydanie kart użytkownikom
- przedłużenie ważności („pieczątka”)
- używanie...
- przedłużenie ważności („pieczątka”)
- używanie...
- ...
- zakończenie wykorzystania legitymacji

Integracja z kartą bezstykową

- jest możliwa i dobra dla lokalnych zastosowań
  - systemy dostępu
  - „karty miejskie” (potencjalny sponsor interfejsu bezstykowego)

Bezpieczeństwo

- czy można podrobić legitymację?
  - czy można „wyprodukować” legitymację dla dowolnej osoby
  - czy można przedłużyć legitymację na kolejny semestr?
- czy można legitymację skopiować?
  - i co to daje?
- dodatkowe zabezpieczenia w karcie
  - nadruk
  - hologramy

Podsumowanie

- jeśli legitymacja będzie wdrażana to...
  - jest to unikalny projekt kartowy
    - wiele typów kart
    - wielu wydawców
    - wiele innych, lokalnych zastosowań (multiaplikacyjność)

Pytania?

poczta elektroniczna: pnazimek@elka.pw.edu.pl

pnazimek@gmail.com

www: http://home.elka.pw.edu.pl/~pnazimek/