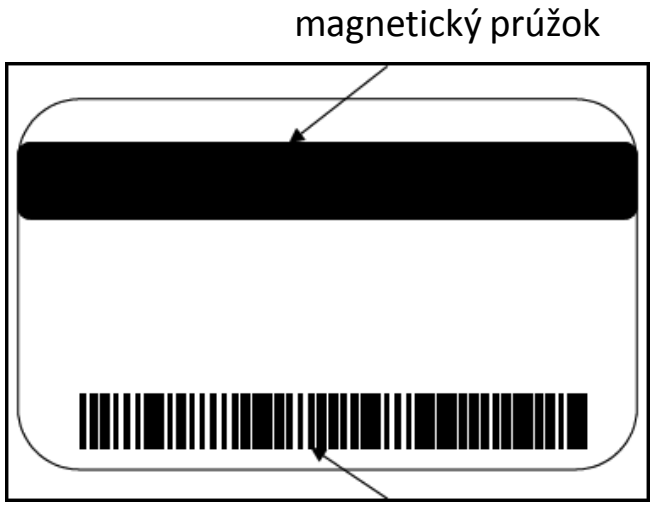
Bezpečnosť informácií na čipových kartách

Čipová karta

Vladimír Hudec, Emtest, a.s. Žilina

Rozdelenie čipových kariet



čiarový kód

QR kód

- Materiál
  - papier
  - plast
- Rozmery
  - ISO 7810 (85,60x53,97x0,76 mm)
- Nosič dát
  - vizuál
    - obrázok, logo, reklama
    - číslo – vytlačené, embosované
  - optický kód
    - 1D kód
    - 2D kód
  - magnetický prúžok

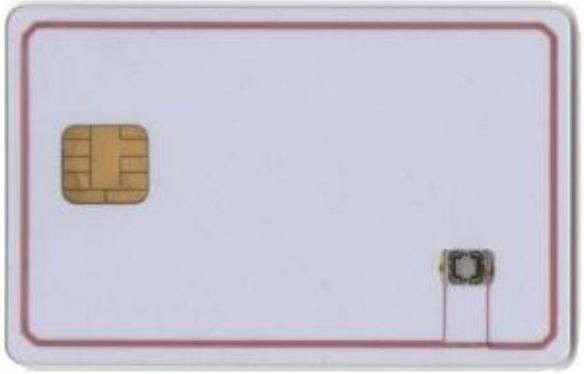
Rozdelenie čipových kariet

kontaktný interface

bezkontaktný interface

- Spôsob komunikácie
  - kontaktné
    - PKI, EMV, SIM, TV, OP, TP ...
  - bezkontaktné
    - EMV, prístup, dochádzka, doprava, ...
  - kombinované
    - duálne
    - hybridné
- Frekvenčné pásmo
  - nízkofrekvenčné
    - 125 kHZ
  - vysokofrekvenčné
    - 13,56 MHZ
  - mikrovlnné

Rozdelenie čipových kariet



hybridná karta

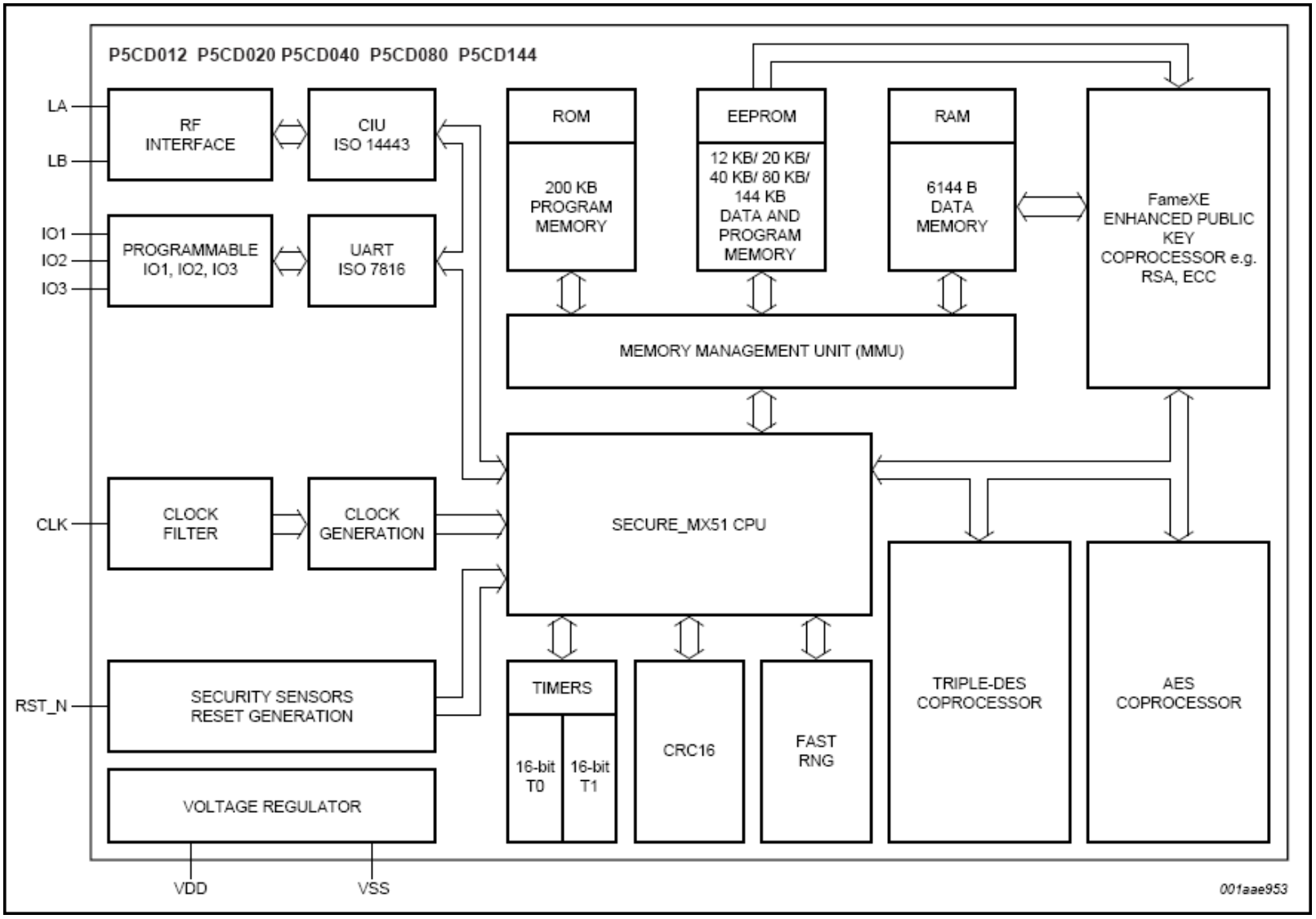
duálna karta

- Prístup k dátam
  - identifikačné
    - identifikátor (číslo)
  - pamäťové
    - bez zabezpečenia prístupu
    - so zabezpečením prístupu
  - procesorové
    - bez koprocesoru
    - s koprocesorom
- Spôsob použitia
  - identifikačné
    - bez zápisu dát na kartu
  - multiaplikačné
    - so zápisom dát na kartu
  - bankové (EMV)

Normy pre čipové karty

- ISO/IEC 7816 – kontaktné karty
  - fyzikálne charakteristiky
  - kontaktný interface
  - prenosový protokol
- ISO/IEC 14443 – bezkontaktné karty
  - fyzikálne charakteristiky
  - RF interface
  - prenosový protokol

Architektúra čipovej karty SmartMX



Bezpečnosť informácií

Informačná bezpečnosť

- Ochrana informačného systému
  - ochrana informácii v ňom uchovávaných, zpracovávaných a prenášaných
- Komunikačná bezpečnosť
  - ochrana prenášaných informácii
- Fyzická bezpečnosť
  - ochrana pred prírodnými hrozbami, fyzickými útočníkmi
- Personálna bezpečnosť
  - ochrana pred vnútornými útočníkmi

Základné princípy bezpečnosti IT

- Integrita dát
  - dáta nemôžu byť ľubovoľne zmenené
- Dôvernosť dát
  - dáta nemôžu byť neoprávnene čítané
- Autentifikácia
  - overenie identity osôb, dát, správ
- Autorizácia
  - overenie oprávnenia osôb, či objektov na prácu s dátami
- Nepopierateľnosť
  - nepopierateľnosť pôvodu dát
  - nepopierateľnosť prenosu a/alebo prijatia dát

Normy pre informačnú bezpečnosť

- ISO 27000
  - séria noriem pre informačnú bezpečnosť
- ISO/IEC 15408 – Common Criteria
  - všeobecný model
    - predmet hodnotenia (TOE – Target of Evaluation)
  - funkčné požiadavky na informačnú bezpečnosť
    - bezpečnostný cieľ (ST – Security Target)
    - profil ochrany (PP – Protection Profile)
  - záruka požiadaviek na informačnú bezpečnosť
    - hodnotenie úrovne zabezpečenia (EAL – Evaluation Assurance Level)
- Global Platform
  - požiadavky na systém pre ČK
    - karta
    - čítačka kariet
    - interface

Bezpečnosť informácií na čipových kartách

Systém čipových kariet

- On-line systém
  - karta = identifikátor majiteľa/držiteľa
    - prístupový, dochádzkový, stravovací, ... systém
    - vernostný systém
- Off-line systém
  - karta = nosič informácii
    - občiansky, vodičský, technický, ... preukaz
    - cestovný pas
    - dopravná karta

Bezpečnostné prvky kartových aplikácii

- Bezpečnosť dát na karte
- Bezpečnosť komunikácie medzi kartou a čítačkou kariet
- Bezpečnosť komunikácie medzi čítačkou kariet a centrálnym systémom
- Bezpečnosť a kontrola dát v centrálnom systéme

Bezpečnosť on-line systému ČK

- Karta je jednoznačný identifikátor jej držiteľa/majiteľa
- Karta okrem identifikátora neobsahuje žiadne ďalšie údaje
- Aplikačná logika je v centrálnom systéme

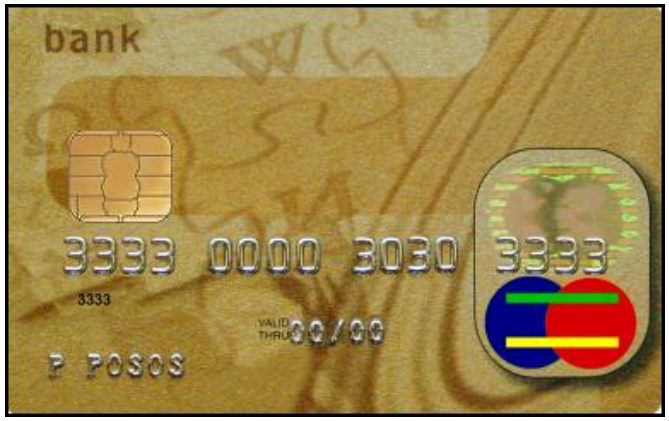
Bezpečnosť off-line systému ČK

- Karta obsahuje aplikačné data
- Aplikačná logika je v čítačke kariet
- Požiadavky na bezpečnosť dát
  - zabezpečený prístup k datam na karte
    - kľúč, PIN, certifikát
  - zabezpečené data na karte
    - kryptografické algoritmy (šifrovanie a/alebo podpisovanie dát)
  - zabezpečená komunikácia
    - šifrovaný prenos dát

Kryptografické algoritmy pre ČK

- Symetrické algoritmy
  - proprietárne
  - 3DES
  - AES
- Asymetrické algoritmy
  - RSA
  - ECC

Štandardy pre aplikácie na ČK



EMV karta

Technický preukaz

- Bankové karty
  - EMV 4.3
- SIM karty
  - ETSI TS 102 221 (GSM 11.11)
- Občiansky preukaz
  - CEN TS 15480
- Vodičský preukaz
  - ISO 18013
- Technický preukaz
  - EU 2003/127/ES

Štandardy pre aplikácie na ČK

Cestovný pas

- Cestovný pas
  - ICAO Doc 9303
- Karta pre elektronický podpis
  - CWA 14890
- Televízna karta
  - EN 50221
- Vernostné karty
  - OMV, Shell, Tesco, ...

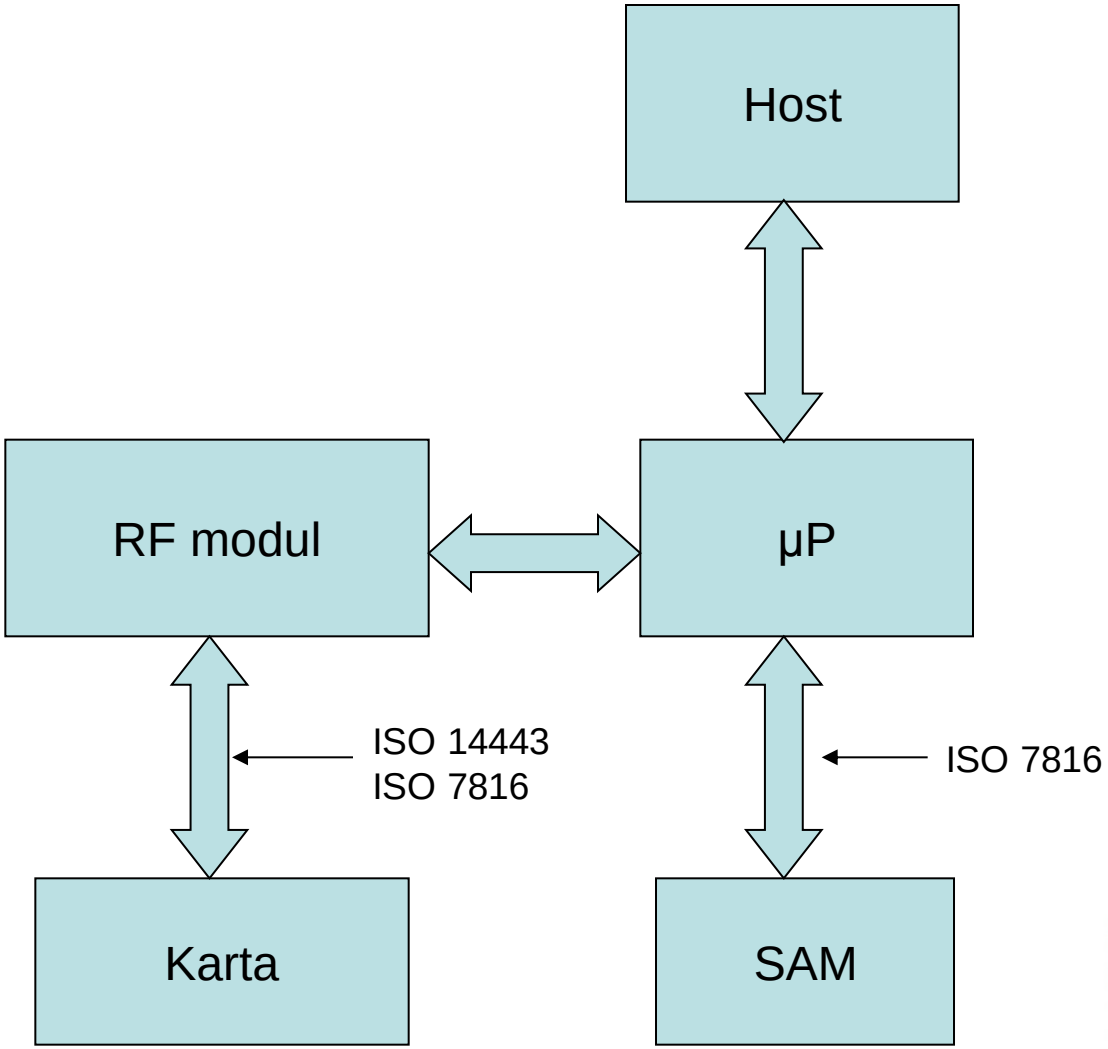
Čipové karty vo verejnej doprave

Data ČK pre verejnú dopravu

dopravná karta

- Predplatný cestovný lístok
  - časová platnosť
  - priestorová platnosť
- Jednorazový lístok
  - kategória cestujúceho
  - platnosť
- Dopravný kredit/peňaženka
  - veľkosť kreditu
- Personálne dáta
  - meno, priezvisko
  - dátum narodenia
- Údaje vydavateľa karty

Čítačka ČK pre verejnú dopravu



Štandardy ČK pre verejnú dopravu

eTicket

- ITSO
  - karty
  - predajné miesta
  - centrálny systém
- Calypso
- VDV KA
  - karta
  - SAM modul
  - procesy pre prácu s kartou
- CIPURSE
  - Open Standard for Public Transport

Dopravné ČK v SR a v ČR

Mifare Classic

- Karta Mifare Classic
  - pamäťová karta
    - 1 kB/4kB
  - jedinečné výrobný číslo
    - 4/7 Byte SNR
  - prístupové kľúče
    - dvojica 48 bitových kľúčov na sektor
  - prístupové práva
    - čítanie a/alebo zápis
  - kryptografický algoritmus
    - Crypto1

Dopravné ČK v SR a v ČR

DESFire karta

- Karta DESFire EV1
  - procesorová karta
    - 2kB/4kB/8kB
  - jedinečné výrobný číslo
    - 7 Byte UID
  - náhodné UID
  - prístupové kľúče
    - 1-15 kľúčov na súbor
  - prístupové práva
    - čítanie a/alebo zápis
  - kryptografický algoritmus
    - 3DES/AES

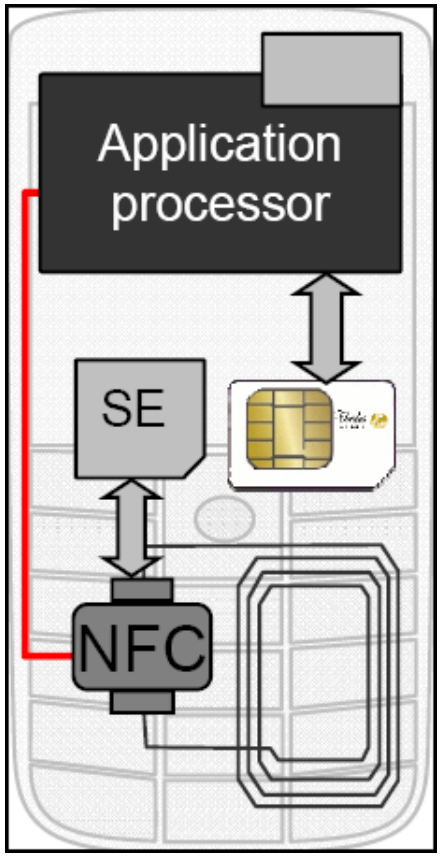
Možné spôsoby narušenie dát na karte

- Narušenie bez priameho finančného prospechu
  - čítanie citlivých (osobných) údajov z karty
  - čítanie identifikátora karty
  - nedostupnosť/zničenie údajov na karte
- Narušenie s priamym finančným prospechom
  - modifikácia údajov na karte
  - klonovanie karty
  - odpamätanie pôvodného stavu karty

Možné spôsoby ochrany dát na karte

- Karta
  - bezpečnostné mechanizmy karty
- Aplikácie na karte
  - diverzifikované prístupové kľúče
  - šifrovanie dát
  - podpisovanie dát
- Architektúra systému
  - správa kľúčov
  - kontrola dát v centrálnom systéme
- Užívateľ
  - obozretné používanie

Ako ďalej ?



NFC mobil

- NFC mobil
  - platobné aplikácie
  - vernostné aplikácie
  - dopravné aplikácie
  - ...

Ďakujeme za pozornosť

EMTEST

eFOCUS