Elektronický cestovní pas

Jan Valášek, FJFI ČVUT

Obsah

1. Starý klasický pas
2. Nový elektronický pas
3. Útoky a obrana
4. Závěr

Starý pas

- Vydáván v ČR do roku 2006
- Ochranné prvky:
  - Speciální papír
  - povrchová ražba
  - vodoznak
  - laserové nápisy
  - Prvky viditelné pod UV
  - bezpečnostní tisk s vícebarevným gravírováním
- Biometrie = fotografie
- => pasivní autentizace
- Automatizace = 2 řádky strojově čitelného textu


12 TITUL / ACADEMIC DEGREE / TITRE
ČESKÁ REPUBLIKA/CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
CESTOVNÍ PAS / PASSPORT / PASSEPORT
CZE
ČESKÁ REPUBLIKA / CZECH REPUBLIC
SPECIMEN


EVROPSKÁ UNIE
EUROPEAN UNION - UNION EUROPÉENNE
ČESKÁ REPUBLIKA
CZECH REPUBLIC - RÉPUBLIQUE TCHÈQUE - TSCHECHISCHE REPUBLIK
CESTOVNÍ PAS
PASSPORT - PASSEPORT - REISEPASS - PASSAPORTO
A10
SPECIMEN


18
VÍZA
VISAS / VISAS
19
VÍZA
VISAS / VISAS
SPECIMEN

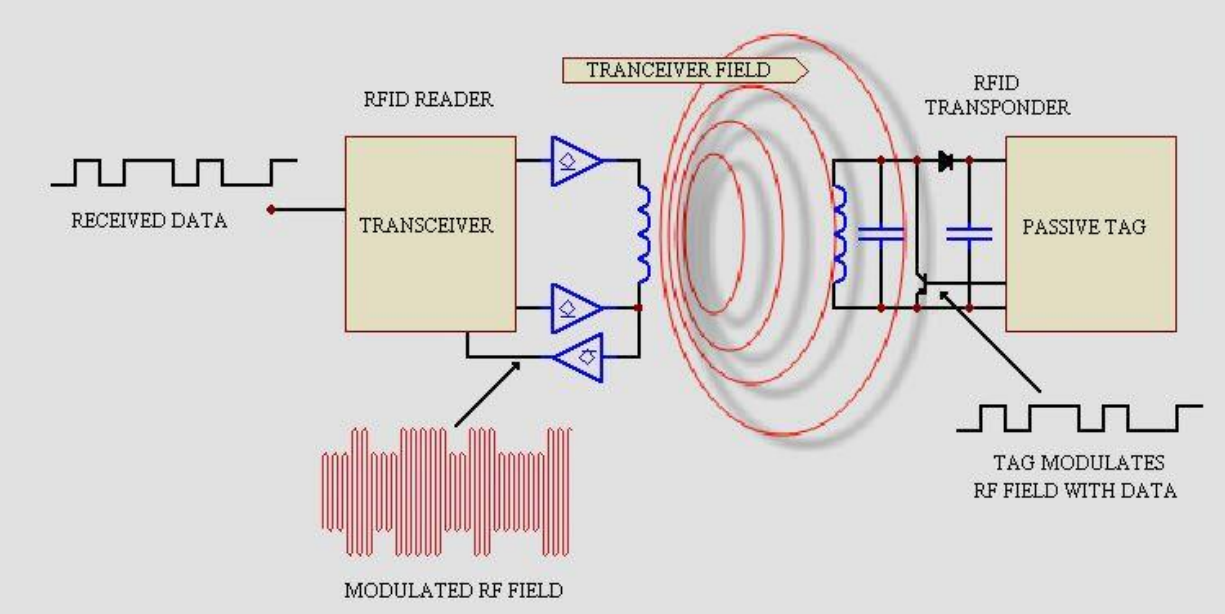
Elektronický pas

- 1. 9. 2006 první pasy s RFID čipy
  - Ty jsou dány ICAO standardy
  - Obsahují pouze snímek obličeje
  - Chráněny pouze BAC
- 28. 6. 2009 i s otisky prstů
  - Přidán protokol EAC

Elektronický pas

- Paměť – EEPROM 72kB
- Rozdělena do 16 segmentů:
- DG1 – stroj. čitelná zóna
- DG2-7 – biometr. data
- DG8-10 – popis bezp. prvků
- DG11 – údaje o majiteli
- DG12 – údaje o vydavateli
- DG13 – interní použití
- DG14 – pro účely EAC
- DG15 – veřejný klíč
- DG16 – příbuzní pro nouzový případ

Elektronický pas



- možnosti odposlechu:
  - aktivní komunikace s pasem - desítky cm
  - odposlech - terminál i pas - jednotky cm
  - odposlech - pouze terminál - desítky m
  - aktivní komunikace s terminálem - desítky m

Útoky a obrany

- Zjištění přítomnosti pasu
  - Hardwarově – přítomnost čipu v EM poli o známých parametrech
  - Softwarově – odpověď na přítomnost pasu
- Možnost zjistit státní příslušnost
  - Nestandardizované chybové hlášky
- => ochranné pouzdro (Faradayova klec)

Útoky a obrany

- Odposlouchávání komunikace
  - Získání biometrických dat?
- => BAC (Basic Access Control)
  - Po úvodní komunikaci přichází ověření
  - Klíč je vytvořen z **čísla pasu**, **data narození** a **data platnosti pasu** = toto se zahašuje pomocí SHA-1
  - Z haše jsou vytvořeny 2 klíče pro 3DES šifru
  - Teoreticky 56bitů, díky malé entropii výrazně méně, cca. 35 bitů
  - >Možný off-line útok

Útoky a obrany

- Okopírování dat na čipu
  - Vytvoření identické kopie?
- => EAC (Extended Access Control)
  - V čipu je uložen soukromý asymetrický klíč - DG14
    - Vydaný Statní tiskárnou cenin - 2056b
    - Neexistuje příkaz na jeho přečtení
  - V čipu je uložen veřejný klíč - DG15
    - Vydaný Ministerstva vnitra s modulem 3072b

Útoky a obrana

- EAC (Extended Access Control)
  - Ověření pomocí protokolu výzva- odpověď
    - Ověření, že čip má k dispozici soukromý klíč odpovídající klíči veřejnému
    - Terminál pošle náhodné číslo, čip pasu doplní další náhodnou částí a digitálně podepíše, terminál podpis ověří
  - Nelze vytvořit nový pár klíčů, neboť veřejný klíč musí být digitálně podepsán vydávající autoritou
  - Slabinou je možnost prodloužení doby na odpověď

Závěr

- Pasy obsahují biometrické údaje
- Lepší identifikace
- Bezpečnost je snad dostatečná
- Budoucnost?

Zdroje

- Časopis Crypto World – články V. Klímy
- http://en.wikipedia.org/wiki/Biometric_passport
- http://www.epassport-book.com/download.php
- http://www.ics.muni.cz/bulletin/articles/534.html
- http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf

Děkuji za pozornost ;)