AR VIEDKARŠU DROŠĪBU SAISTĪTIE ASPEKTI

Juris Pūce, CISA
Analytica
ISACA rudens konference 2012

analytica

Tehnoloģijas un lietojumi

- Atmiņas karte (mazas ietilpības)
- Aizsargāta čipkarte
- Bezkontakta karte
- Kombinētie varianti
  - Hibrīdā karte
  - Duālā karte

Tipiskākie lietojumi

- Bankas kartes (pārsvarā kontakta)
- Visas pilsoņu “jaunās/sarkanās” pases = bezkontakta
- eID karte = hibrīdā karte
- E-talons = bezkontakta karte (RFID)
- Elektroniskā paraksta viedkarte
- SIM kartes telefonos
- Satelīta televīzija

- Dažāda veida autentifikācijas kartes

Aktuālās tehnoloģijas no drošības viedokļa (buzzwords)

- Viedkartes (drošās)
  - ISO/IEC 7810 un ISO/IEC 7816
  - Procesors, datu glabātuve un aplikācijas uz kartes
- RFID un NFC tehnoloģijas
  - Dažādi standarti
  - Divvirzienu komunikācija
  - Procesors, datu glabātuve, aplikācijas

Sašaurinam mērogu

- Elektroniskās identifikācijas viedkaršu drošība
- Bezkontakta tehnoloģiju drošība
- Kontakta tehnoloģiju drošība

- Neaiztiekam
  - Banku kartes šoreiz ☺
  - Magnētiskās kartes

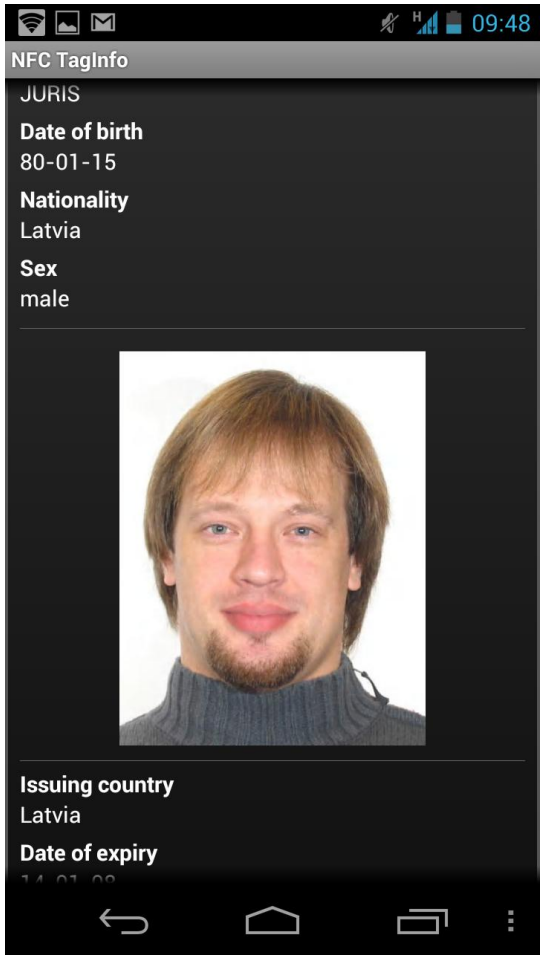
KĀDĒĻ MĒS IZMANTOJAM VIEDKARTES?

Apdraudējumi bezkontakta tehnoloģijām

- Izmantojam tipiski:
  - Piekļuves kontrolei
    - MifareClassic
  - Sabiedriskajam transportam
    - Vienreizlietojamas un daudzkārtlietojamas
  - Topošais (esošais?) norēķinu lietojums (NFC)
- Mašīnlasāmi ceļošanas dokumenti (ICAO)
  - Katrs var pats nolasīt savā pasē esošos pamatdatus jau šobrīd

- Daži piemēri izdomai…

Pase


09:48
NFC TagInfo
JURIS
Date of birth
80-01-15
Nationality
Latvia
Sex
male
Issuing country
Latvia
Date of expiry


09:48
NFC TagInfo
EF.DG1: Machine-readable Zone Data
MRZ data elements
Tag: 5F1F
Length: 88 Byte
Encoding: US-ASCII
P<LVAPUCE<<JURIS<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<LV33567358LVA8001151M1401084150180<123
01<<08
Back

TAD VARBŪT IZMANTOJAM TIKAI ČIPKARTES?

Apdraudējumi kontakta tehnoloģijām

- Neautorizētas aplikācijas
- Kļūdas aplikācijās un dizainā
- Fiziskā lietošana kombinācijā ar datoru
- Fiziska uzlaušana

Apdraudējumu sekas

- Karšu satura un iespējams karšu klonēšana
- Mērķētu uzbrukumu koncepcija

Tipisks lietojums, kas vēl pieaug

- Kombinēta lietošana organizācijās
  - Hibrīda kartes fiziskās, IT infrastruktūras un aplikāciju piekļuves kontrolei

Par lietošanu no drošības viedokļa

- Balts
  - Dažādi lietojumi
  - Digital Identity?
  - Divi faktori – teorētiski drošāk…
  - Papildus elektroniskie lietojumi (šifrēšana, parakstīšana, piekļuve dažādām aplikācijām, piekļuve tīklam)
  - Papildus praktiskie lietojumi (ID karte, Piekļuves kontrole)
  - Precīzāka kontrole

- Melns
  - Tehniski sarežģītāk (dārgāk…)
    - Viedkartes
    - Klienta aplikācijas (integrēts/neintegrēts)
    - Izsniegšanas process (dzīvescikls)
  - Citi riski
    - PIN / Keylogging
    - Nodod citam ar visu PIN
    - PIN on card
    - Šifrēšanas un parakstīšanas blakusefekti… (HSM)

Kas vēl ir iespējams. Būs?

- OTP papildus
- Biometrija integrēta
  - ES normatīvi par biometrijas datu glabāšanu
- Integrētas aplikācijas uz kartēm
  - Pārlūkprogrammas piemērs

Čipkartes uzlaušana

Paldies

- juris.puce@analytica.lv