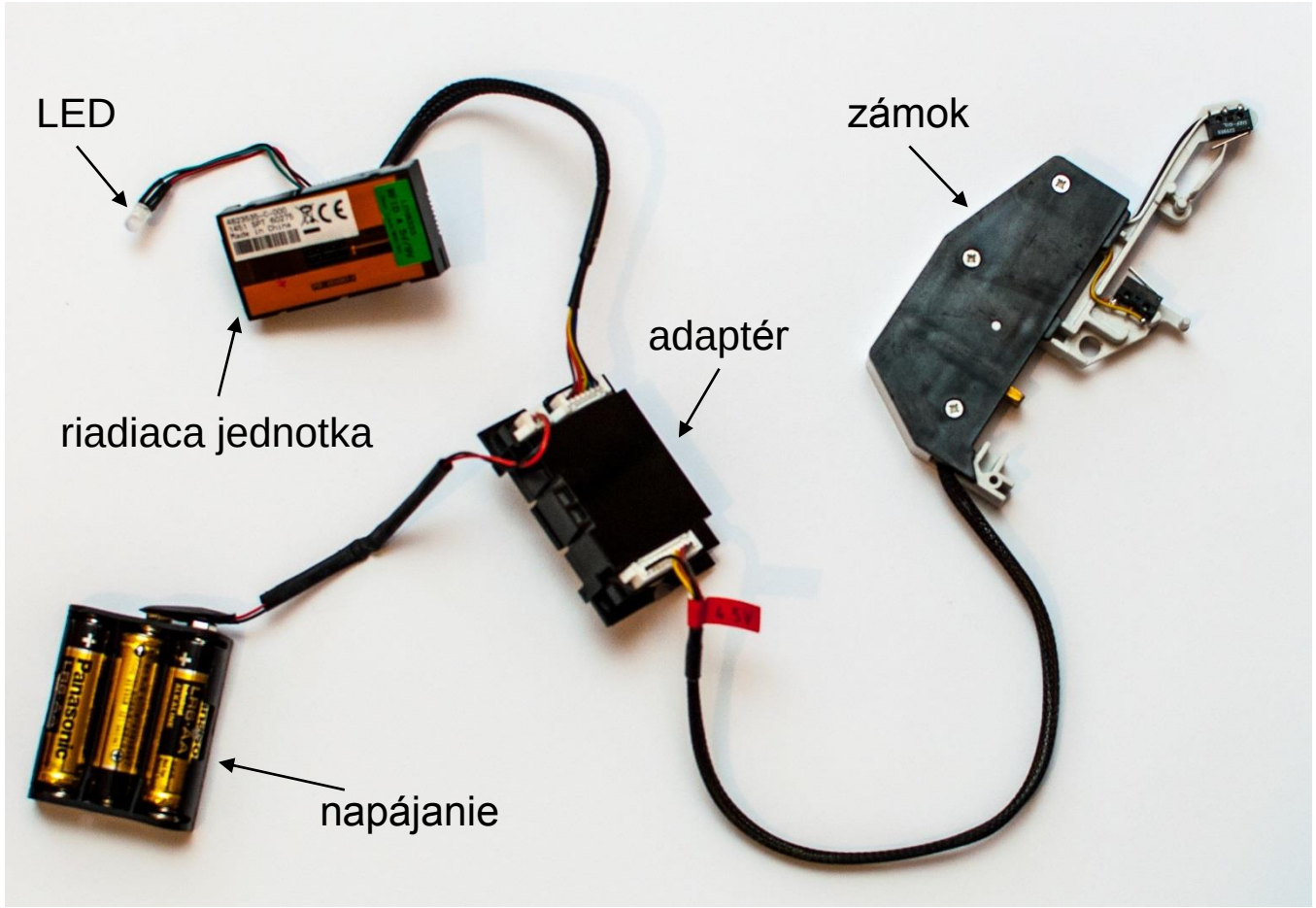
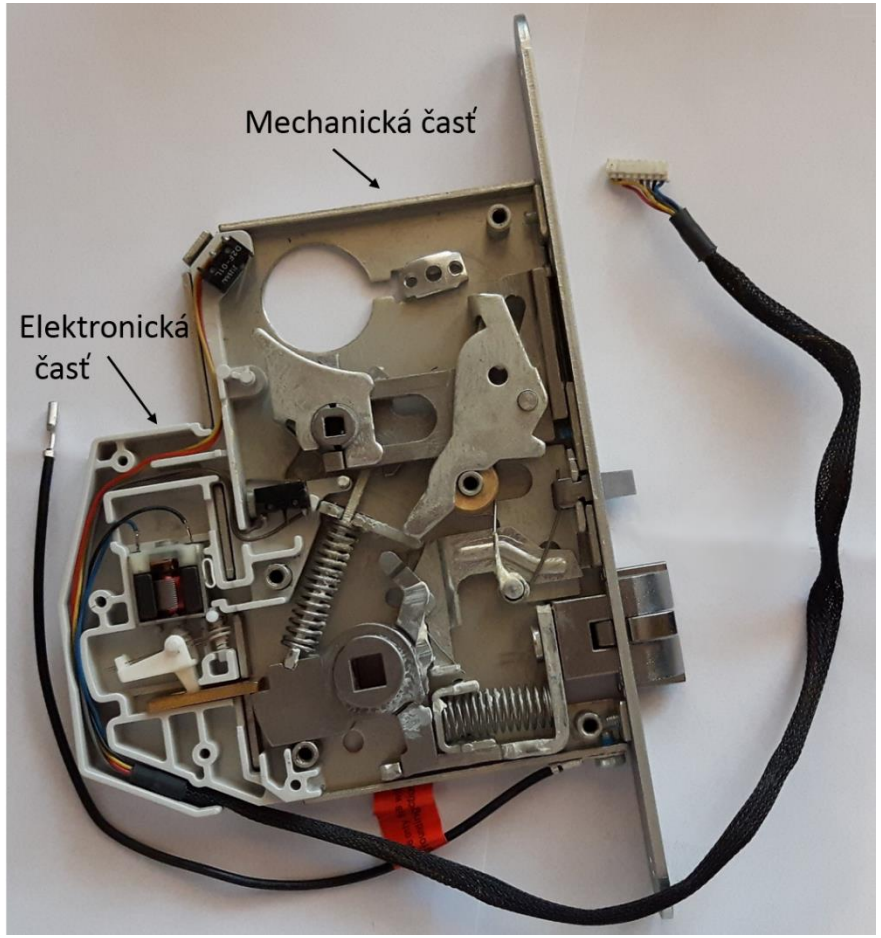
Analýza bezpečnosti hotelového systému využívajúceho RFID karty

Bc. Veronika Mečiarová

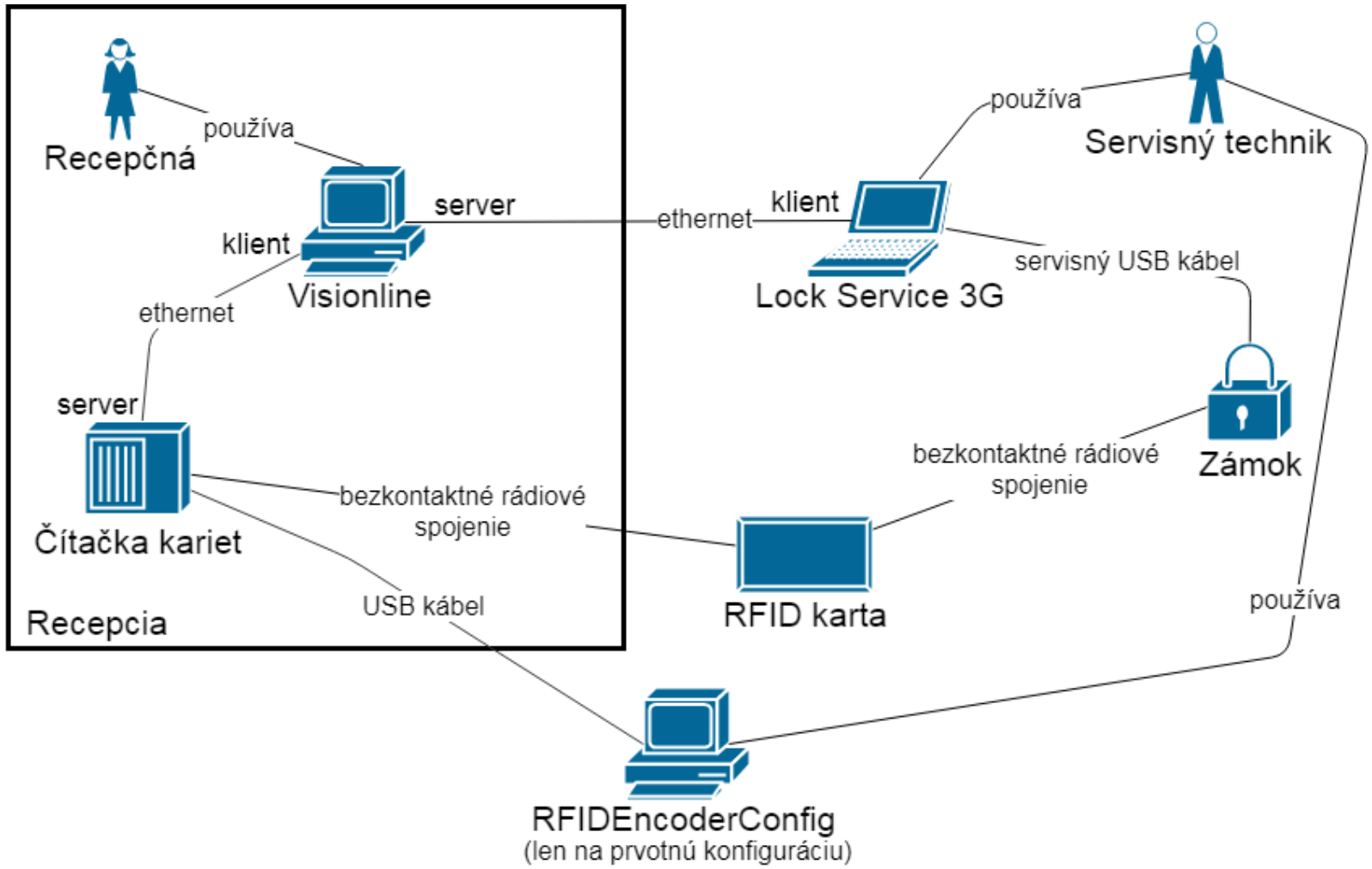
Školiteľ: RNDr. Richard Ostertág, PhD.
Konzultant: Mgr. Peter Košinár

Analyzované zariadenie



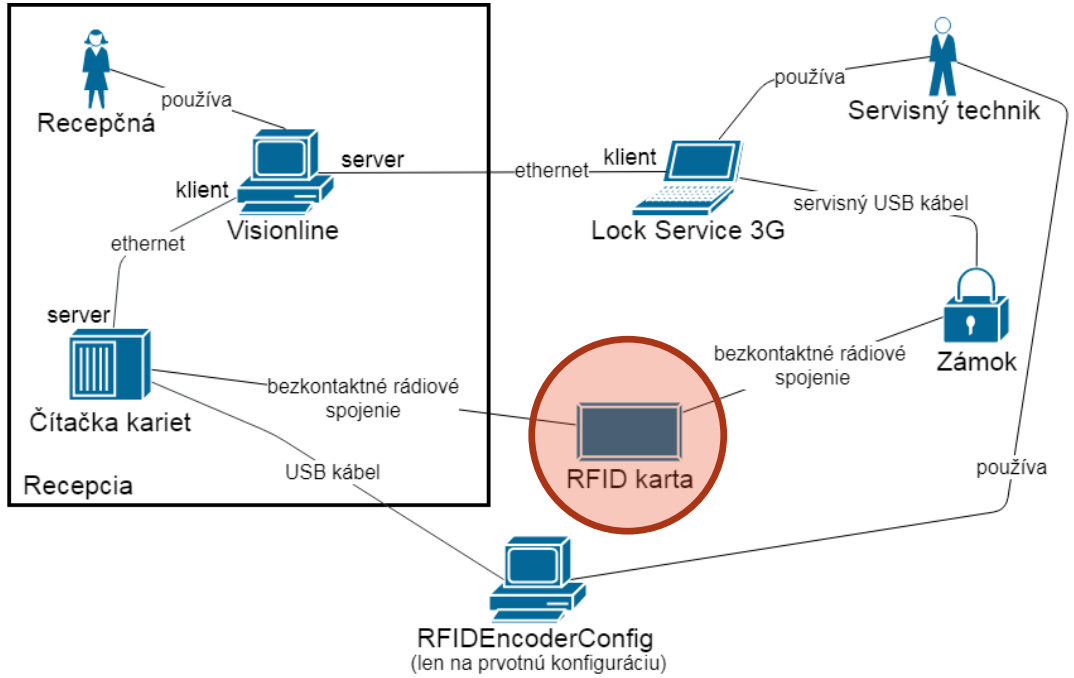


Analyzované zariadenie



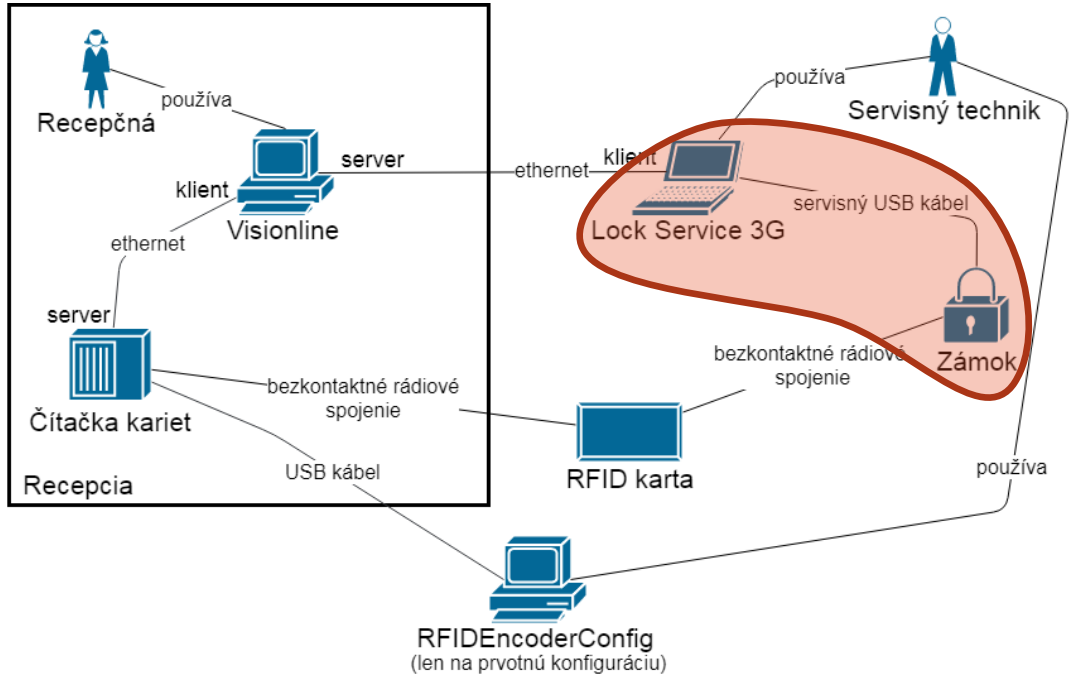
Cieľ práce

- analýza bezpečnosti prístupového systému
  - karty RFID



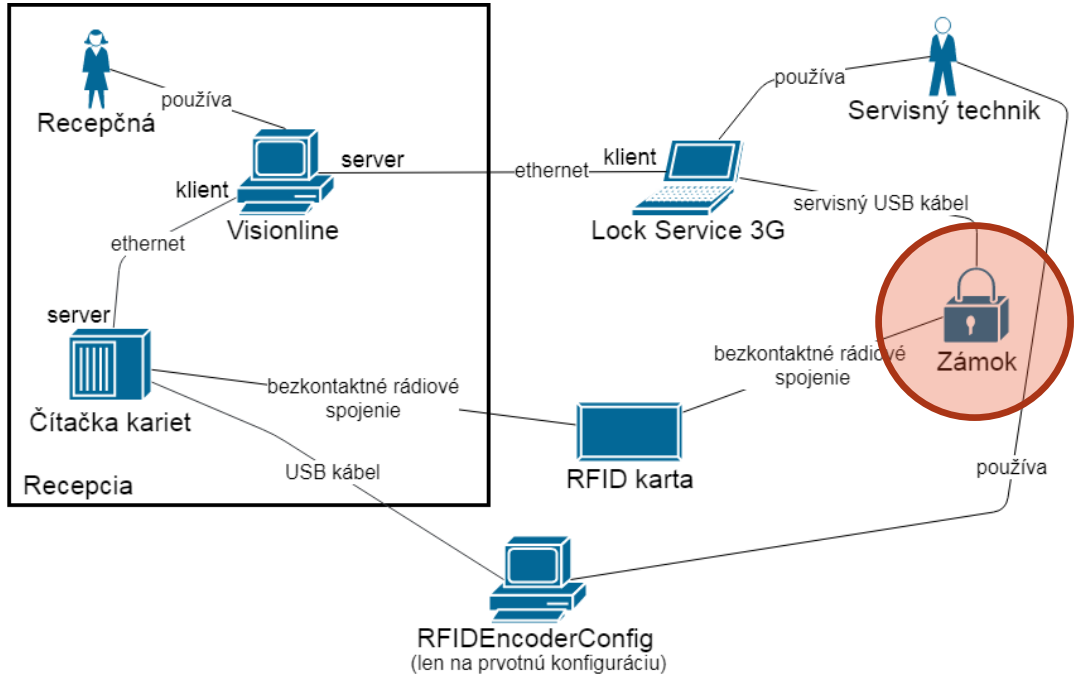
Cieľ práce

- analýza bezpečnosti prístupového systému
  - karty RFID
  - komunikácia servisného počítača so zámkom



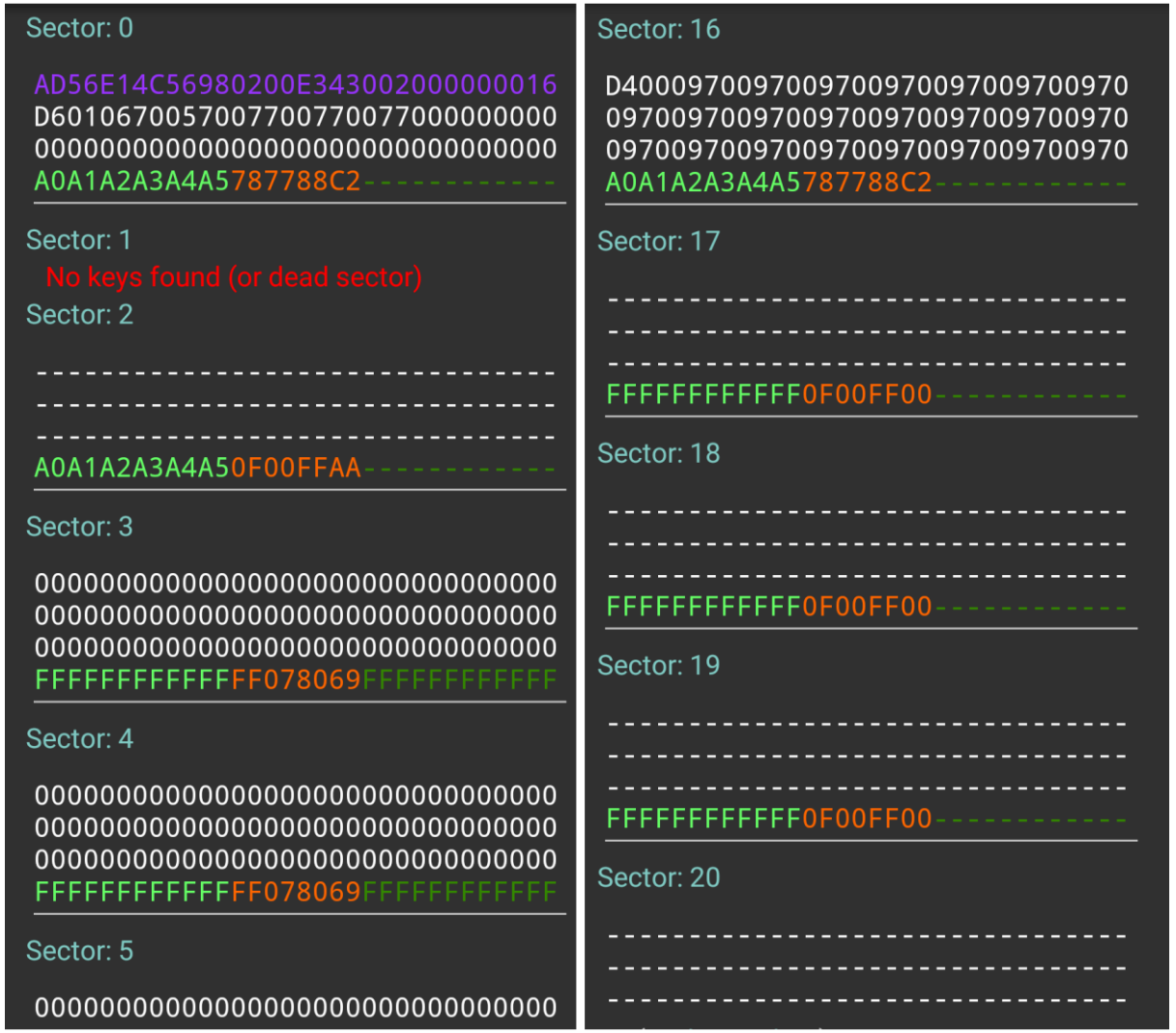
Cieľ práce

- analýza bezpečnosti prístupového systému
  - karty RFID
  - komunikácia servisného počítača so zámkom
  - firmvér zámku



Bezpečnosť kariet

- Mifare Classic 4K
  - 40 sektorov
    - 32 sektorov – 4 bloky
    - 8 sektorov – 16 blokov
  - 1 blok = 16B
  - kľúč A, B
  - prístupové práva
  - prenosový protokol CRYPTO1



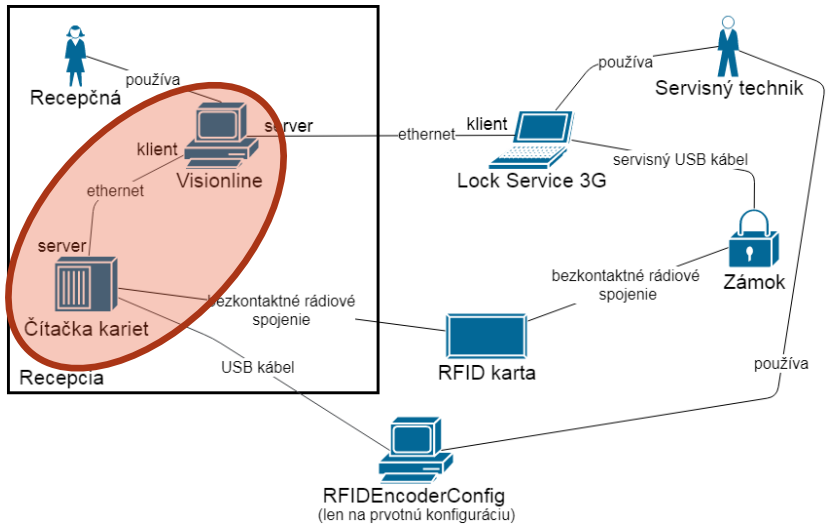
Bezpečnosť kariet

- získanie kľúčov
  - **štandardné kľúče**: 0xA1A2A3A4A5, 0xFFFFFFFFFFFF

Bezpečnosť kariet

- získanie kľúčov
  - **štandardné kľúče**: 0xA1A2A3A4A5, 0xFFFFFFFFFFFF
  - **odpočúvanie komunikácie** počítač ↔ čítačka

```
410111 47f9ed23756 ded1e1c7c00000000
41000200ed1e1c7c18110a171e01070d6500b4bc700186c60000697785096aae0101001e005f7f3eda608858b2c78192ade3c148583af8bb
2d0000000000000f00ff00000000000000
410112 47f9ed23756 ded1e1c7c00000000
41000200ed1e1c7c1831d8efa51f03ffa0a048e20ce92b112c51c67d919897021338c9a38dadaee91b8c953e53c906988933d31ea1d3b057
a60000000000000f00ff00000000000000
```



Bezpečnosť kariet

- získanie kľúčov
  - **štandardné kľúče**: 0xA1A2A3A4A5, 0xFFFFFFFFFFFF
  - **odpočúvanie komunikácie** počítač ↔ čítačka

```
4101114 7f9ed23756ded1e1c7c00000000
41000200ed1e1c7c18110a171e01070d6500b4bc700186c60000697785096aae0101001e005f7f3eda608858b2c78192ade3c148583af8bb
2d0000000000000f00ff00000000000000
4101124 7f9ed23756ded1e1c7c00000000
41000200ed1e1c7c1831d8efa51f03ffa0a048e20ce92b112c51c67d919897021338c9a38dadaee91b8c953e53c906988933d31ea1d3b057
a60000000000000f00ff00000000000000
```

  - **hardnested útok**
    - Proxmark
    - znalosť aspoň jedného kľúča – vnorená autentifikácia
    - slabosť šifry CRYPTO1

Bezpečnosť kariet

- použité sektory: 0, 16 – 39
- obsah čiastočne šifrovaný
- 8B bloky → bloková šifra?

- klonovanie kariet
- zmena obsahu

Bezpečnosť kariet

Dosiahnutie vyššej bezpečnosti:

- náhodné kľúče
- šifrovaná komunikácia
- iný typ kariet
  - bez CRYPTO1
  - Mifare DESfire, Mifare Plus

USB komunikácia so zámkom

- Lock Service ↔ zámok
  - konfigurácia
  - funkcia „Power open“ – vynútenie otvorenia

1. PC pošle zámku:

```
1002 000060ffff1010 81 3279b9690a380dfda7268b58a0053eeeebad21 1003
```

2. zámok pošle:

```
1002 000030ffff1010 81 db5bdbf6941bf10dbe67dc7bf70e15de7f856b4ee2b5aaf1fbebb451e9f0b1e9b014f8 1003
```

3. PC ukončí komunikáciu:

```
1002 000c0c 1003
```

USB komunikácia so zámkom

- bloková šifra Blowfish v 8B CBC móde
- rovnaká dĺžka správ
- inicializačný bajt → inicializačný vektor
- obojsmerne rovnako šifrované
- jednoduchý kľúč
  - reverzná analýza kódu
  - slovníkový útok

1002000060ffff1010	4d	20720665e4a39685d15fc0a585a49fb0783918	10031002000c0c1003
1002000060ffff1010	fc	9fec325b06101016c956947587dfcfc68e95190d	10031002000c0c1003
1002000060ffff1010	40	198f933fc5a169abf8a6b36b0bdf6255358bbf	10031002000c0c1003
1002000060ffff1010	40	198f933fc5a169abf8a6b36b0bdf6255358bbf	10031002000c0c1003
1002000060ffff1010	1f	f33dfbfe9ff46c0ea9c6e73329af7aa23dc23f	10031002000c0c1003
1002000060ffff1010	80	192cb9c7e1ed82c3275cdb396aed4ccdbde872	10031002000c0c1003
1002000060ffff1010	83	a806e354306d4ff2835fe5e21010b91e858efe55	10031002000c0c1003
1002000060ffff1010	e6	131a037cd9c4608817ced87c2caceacd028cdb	10031002000c0c1003

USB komunikácia so zámkom

- málo užitočného obsahu
  - 6B kód inštrukcie
  - kontrolné súčty
  - riadiace bajty
- neobsahuje žiaden identifikátor
- zopakovanie odpočutej komunikácie

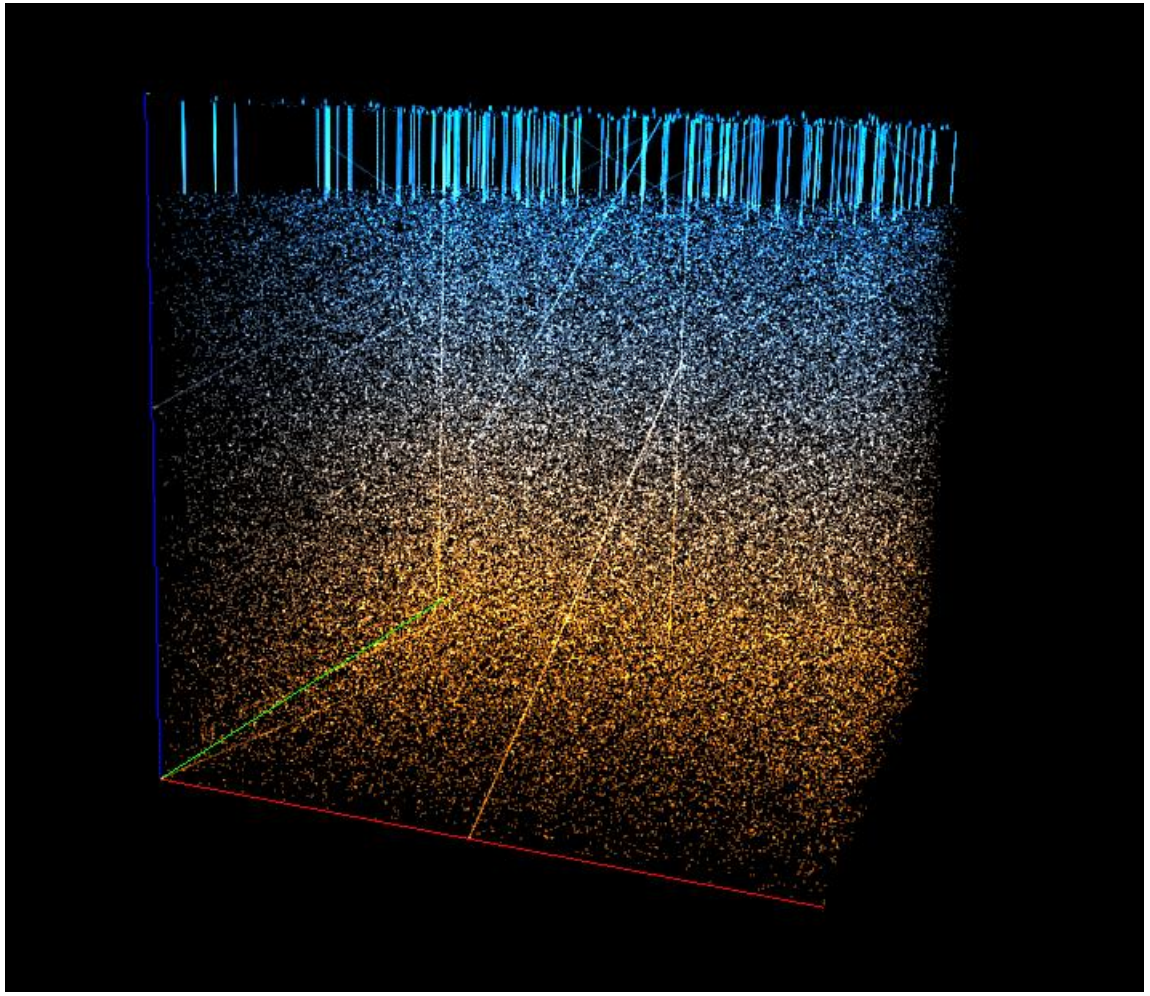
USB komunikácia so zámkom

Dosiahnutie vyššej bezpečnosti:

- nepredikovateľný inicializačný vektor
- rôzne kľúče

Firmvér zámku

- niekoľko rôznych verzií k dispozícii
- veľkosť 121 362 B
- štruktúra – 133B bloky (128B dát)



Záver

- **karty**
  - prečítanie obsahu
  - klonovanie
- **komunikácia počítača so zámkom**
  - otvorenie zámku bez použitia karty a aplikácie
- **firmvér zámku**
  - štruktúra
  - možnosť ďalšej analýzy

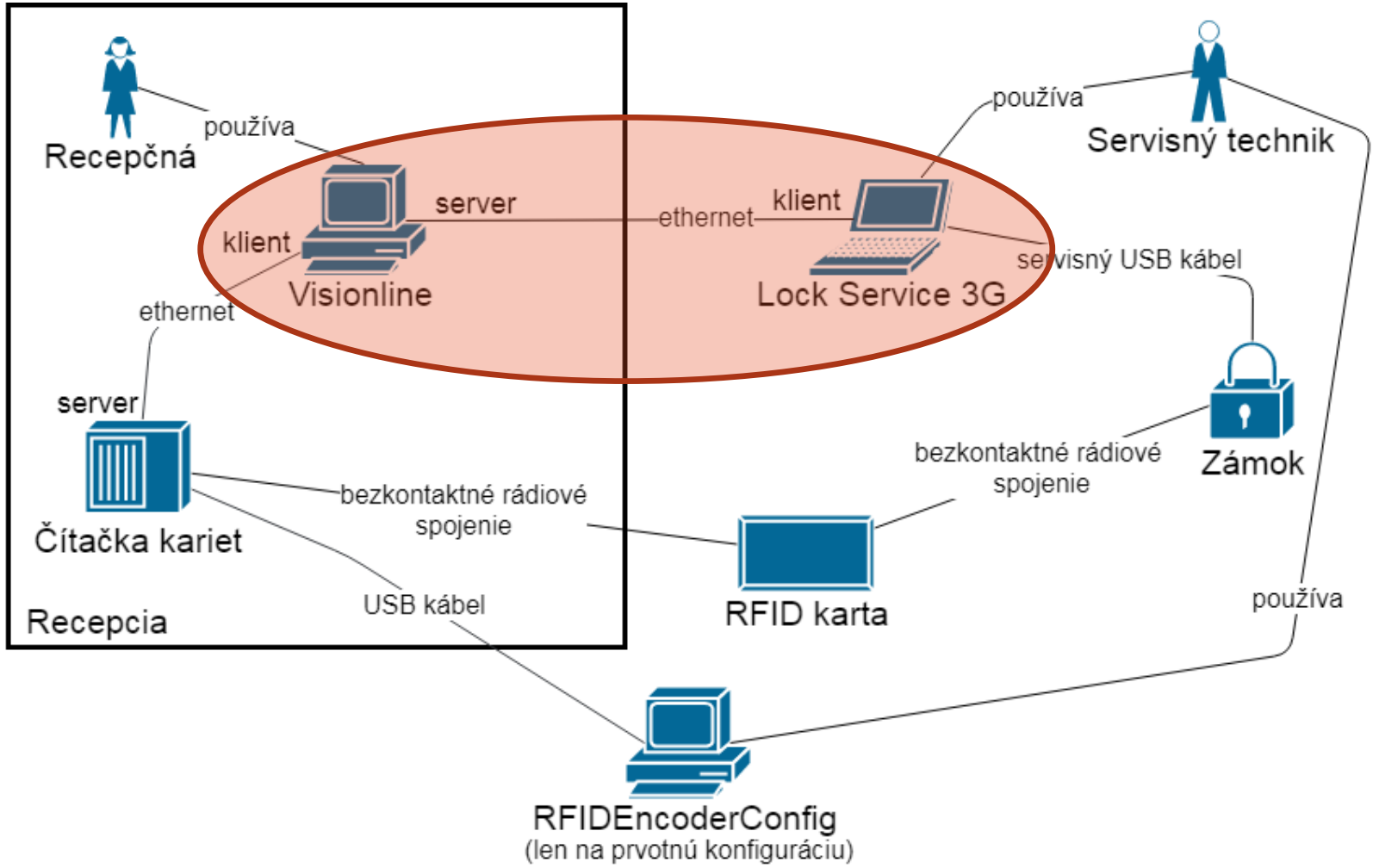
Ďakujem za pozornosť!

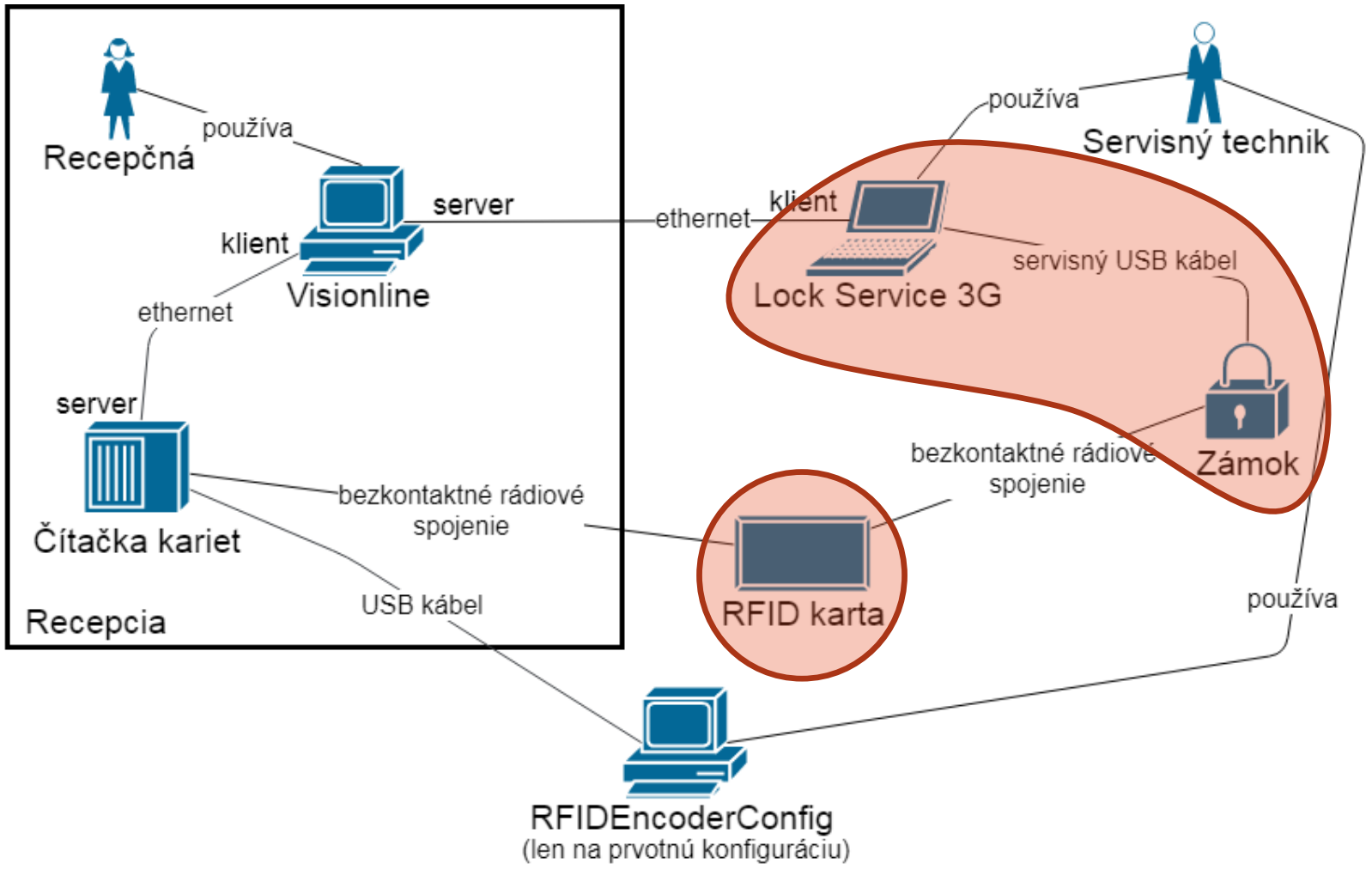
Priestor na Vaše otázky

„Karta typu MIFARE Classic 4K je navrhnutá v súlade so štandardom ISO/IEC 14443. Norma ISO / IEC 14443 je štvordielna medzinárodná **norma pre bezkontaktné čipové karty s krátkym vzdialenostným dosahom**.“

ISO / IEC 14443: Identification cards — Contactless integrated circuit cards — Proximity cards

- Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s těsnou vazbou
- karty s dosahom do 50 cm


Recepčná
používa
server
klient
Visionline
ethernet
klient
Lock Service 3G
používa
Servisný technik
servisný USB kábel
ethernet
server
Čítačka kariet
bezkontaktné rádiové
spojenie
USB kábel
Recepcia
RFID karta
bezkontaktné rádiové
spojenie
Zámok
používa
RFIDEncoderConfig
(len na prvotnú konfiguráciu)


Recepčná
používa
server
klient
Visionline
ethernet
server
Čítačka kariet
bezkontaktné rádiové spojenie
USB kábel
Recepcia
ethernet
klient
Lock Service 3G
používa
Servisný technik
servisný USB kábel
Zámok
bezkontaktné rádiové spojenie
RFID karta
používa
RFIDEncoderConfig
(len na prvotnú konfiguráciu)