Zabezpečenie bezdrôtových komunikačných sietí v inteligentných domácnostiach proti kybernetickým útokom

Bc. Lukáš Doubravský

14. 06. 2017

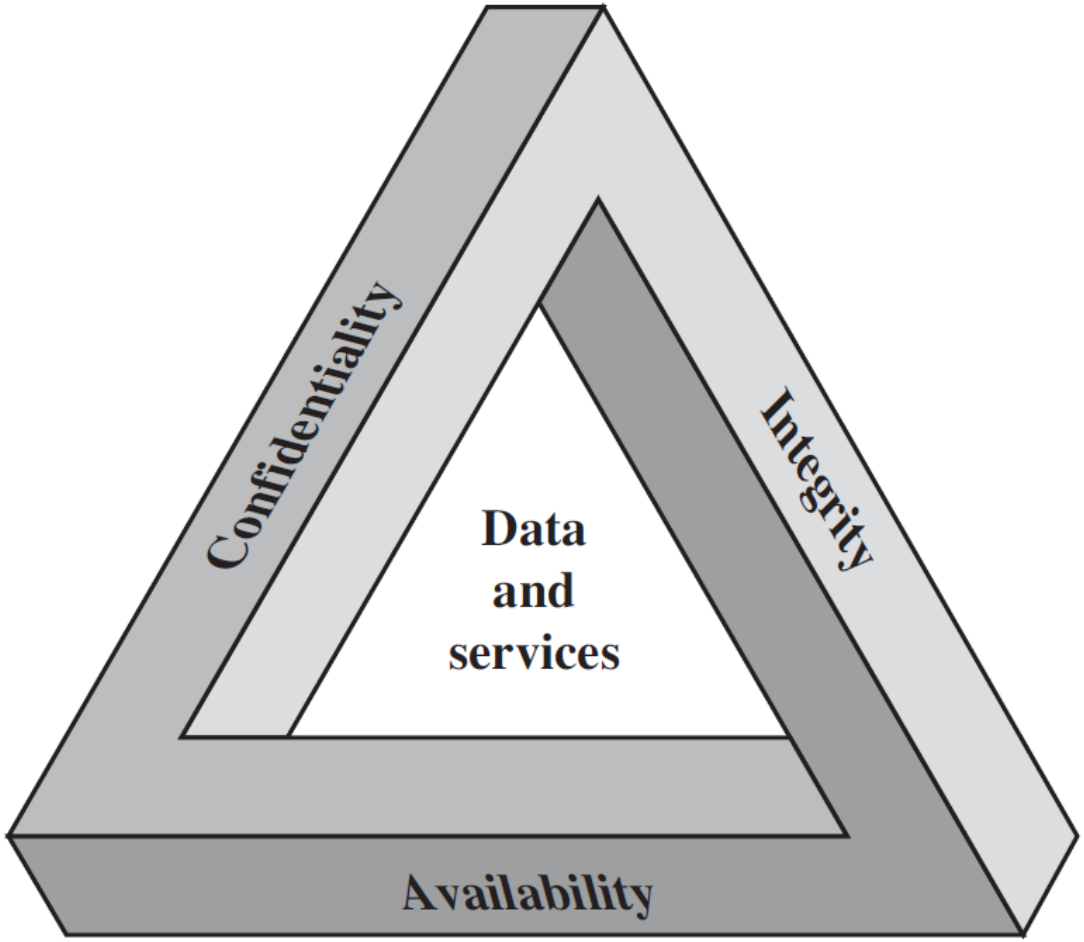
Motivácia

- Bezpečnosť je hra na mačku a myš

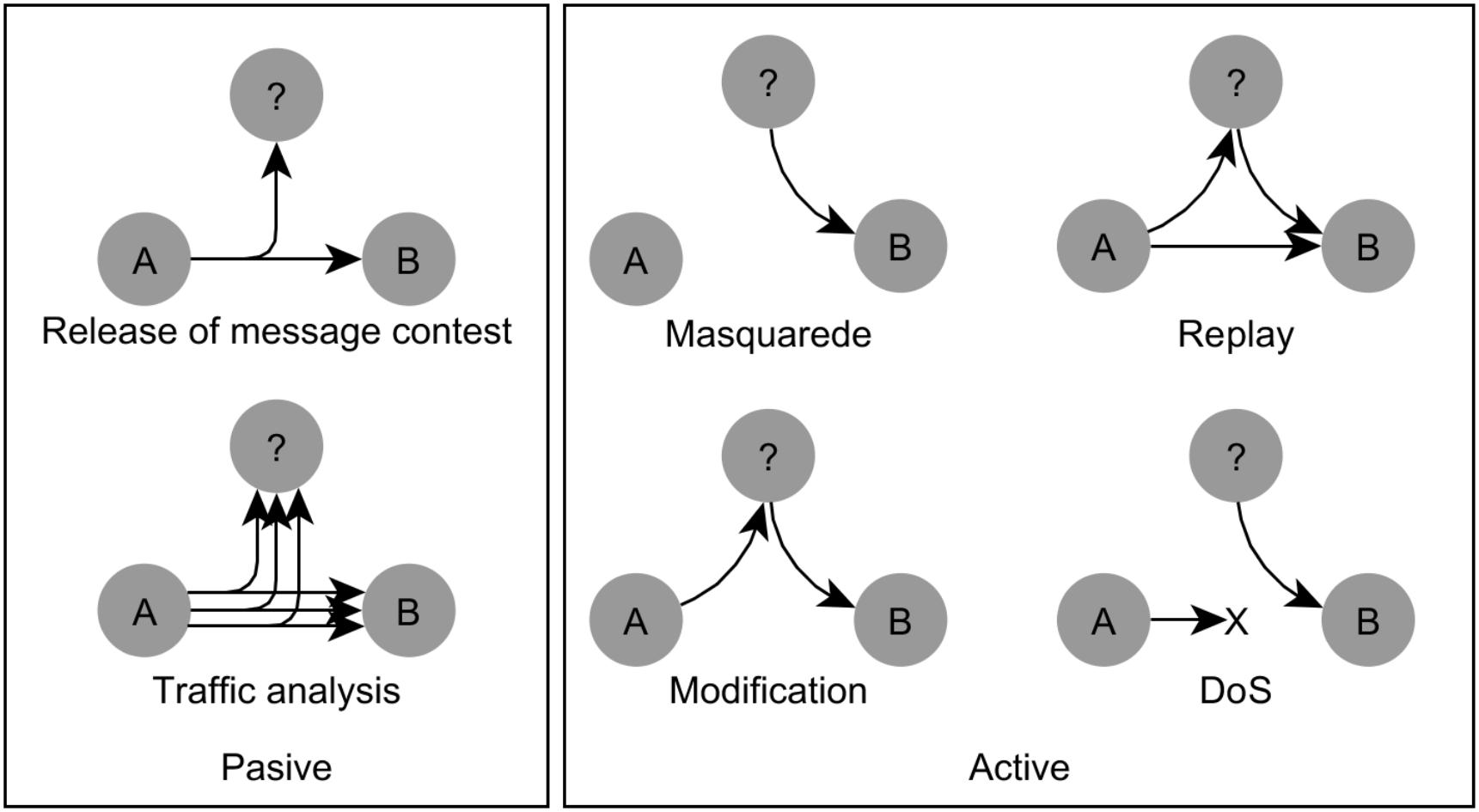
- bezpečnejšie,
- efektívnejšie,
  - spotreba,
  - rýchlosť.

- 8-bitové zariadenia, inteligentná domácnosť

Informačná bezpečnosť



Typy útokov


?
A
B
Release of message contest
?
A
B
Traffic analysis
Pasive
?
A
B
Masquarede
?
A
B
Replay
?
A
B
Modification
?
A
X
B
DoS
Active

Aktuálny stav vo WPAN 802.15

- Zabezpečenie na transportnej ale aj aplikačnej vrstve

- ANT: AES-128
- Bluetooth: AES-CMAC (128)
- Zigbee: AES-128
- LoRaWAN: AES-128

Navrhnuté riešenie

- **HW**
  - kryptolementy

- Zabezpečiť komunikáciu medzi:
  - senzorom,
  - najbližším zariadením s výpočtovým výkonom (cloud, HUB)

Navrhnuté riešenie

- centralizované riešenie,
- PKI
  - RSA/ECC-AES + podpisové schémy
  - Certifikáty (ale predzdieľané “bezpečne” NFC)

- Autentifikáciu na aplikačnej vrstve
  - ostatné aspekty inf. bezp. sa dajú zebezpečiť nad touto vrstvou

- porovnané nezabezpečené riešenie, HW a SW zabezpečenie

Implementácia: Komunikačný protokol

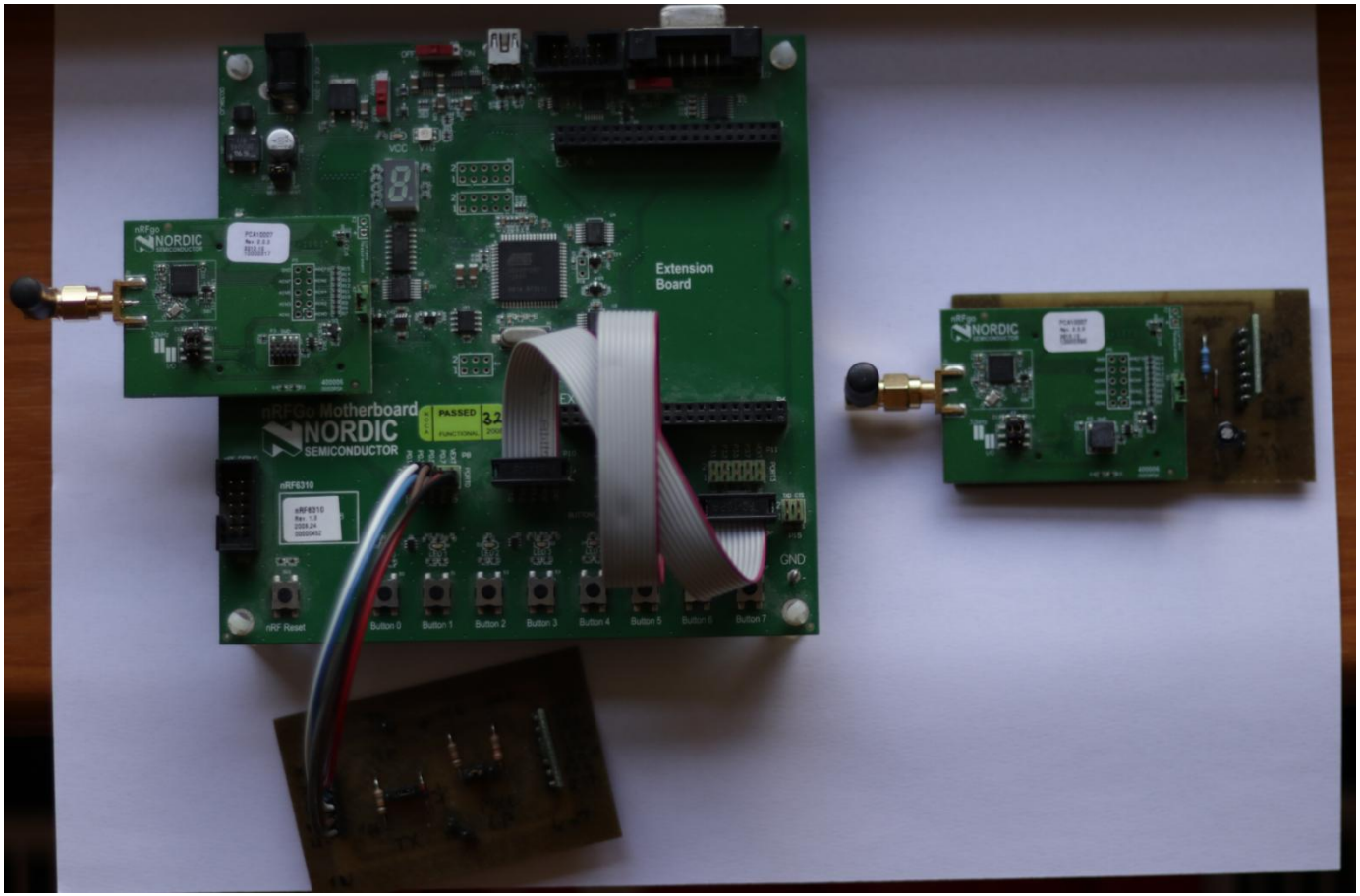
- DK Nordic Semiconductors nRF51422
  - C
  - ANT SoftDevice, 2.4 GHz
  - 32bit architektúra
  - 256 kB program, 16kB RAM

- Medzi 2 zariadeniami

- Zariadenie “Master” je osadený na NRF MotherBoard tlačidlá, LED, nastavuje zabezpečenie
- Zariadenie “Slave“ prispôsobuje zabezpečeniu podľa prijatých správ, dekóduje, zakóduje a posiela naspäť

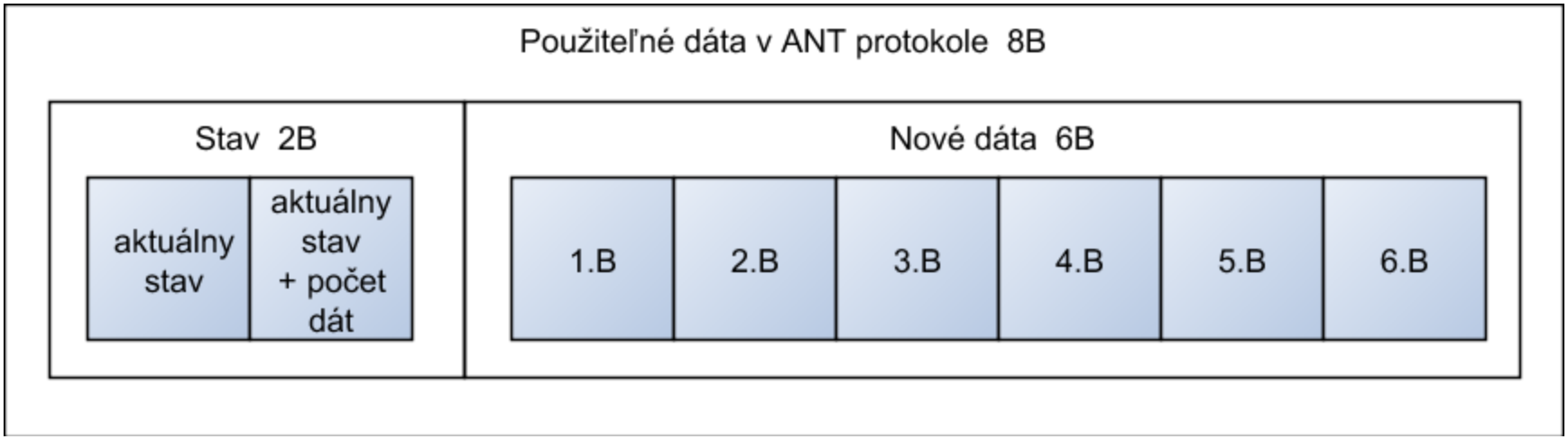
Implementácia: RF komunikácia

TODO better photo



Implementácia: Segmentácia správ

- Viac ako 8 bajtov, maximálne 254 bajtov



- Príklad správ
  - FF FF prázdna správa
  - 00 00 prázdna správa
  - 01 03 01 FF nezabezpečená správa
  - 03 03 prázdna správa

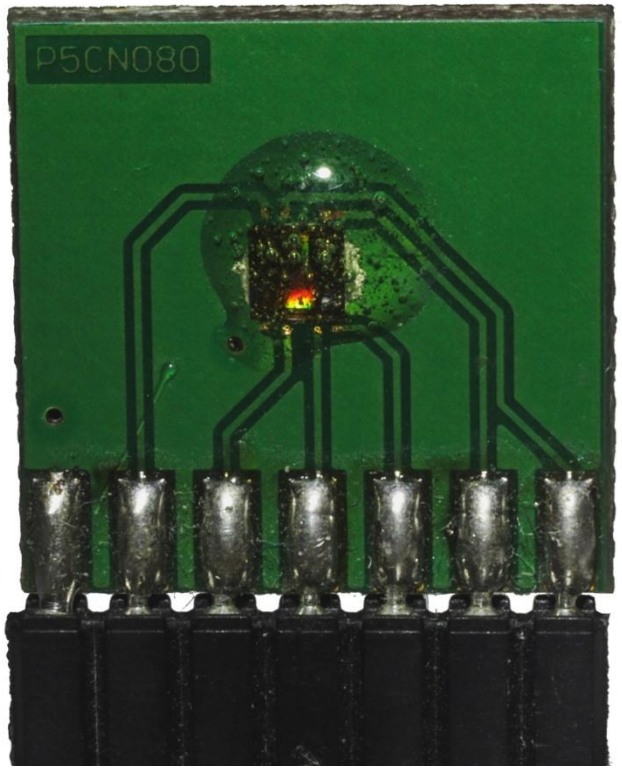
Implementácia: SW AES

- Referenčná implementácia
- TinyAES-128 C
- CBC

- Použitie viac-menej priamočiare

Implementácia: HW AES

- Secure element
- HW: NFC, RNG, RSA, ECC, AES, DES koprocesor apod.



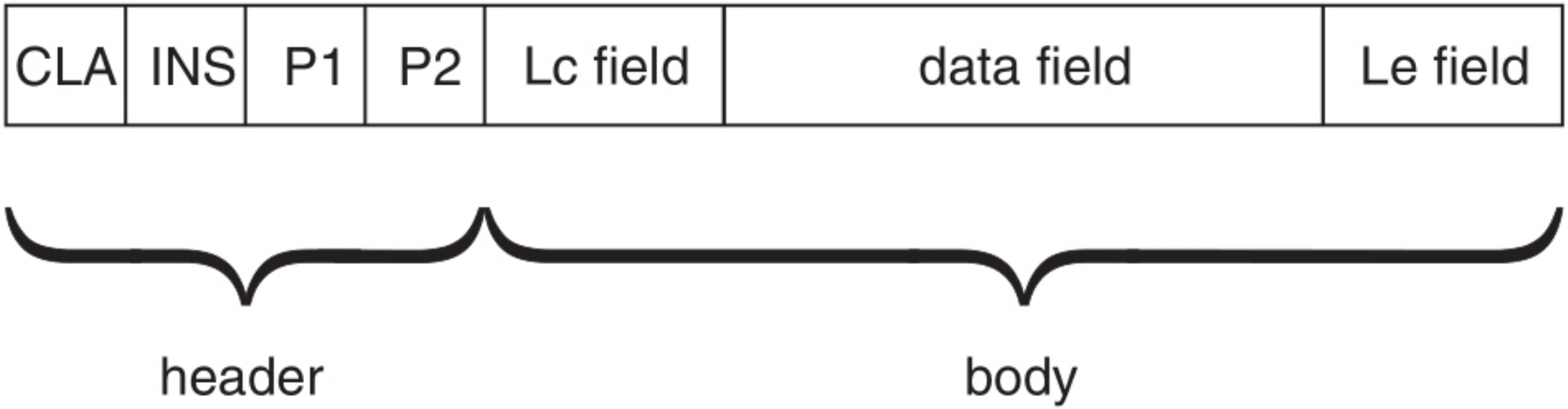
Implementácia: ISO7816

- Signály sú generované GPIO a HW periférií (*PPI*)
- IO signál UART
  - 2.667 MHz
  - 7168 bps

- ATR (answer to reset), nastavenie časovanie

- Komunikácia
  - T=0 bajtová APDU
  - T=1 bloková APDU zabalené do bloku
- LRC

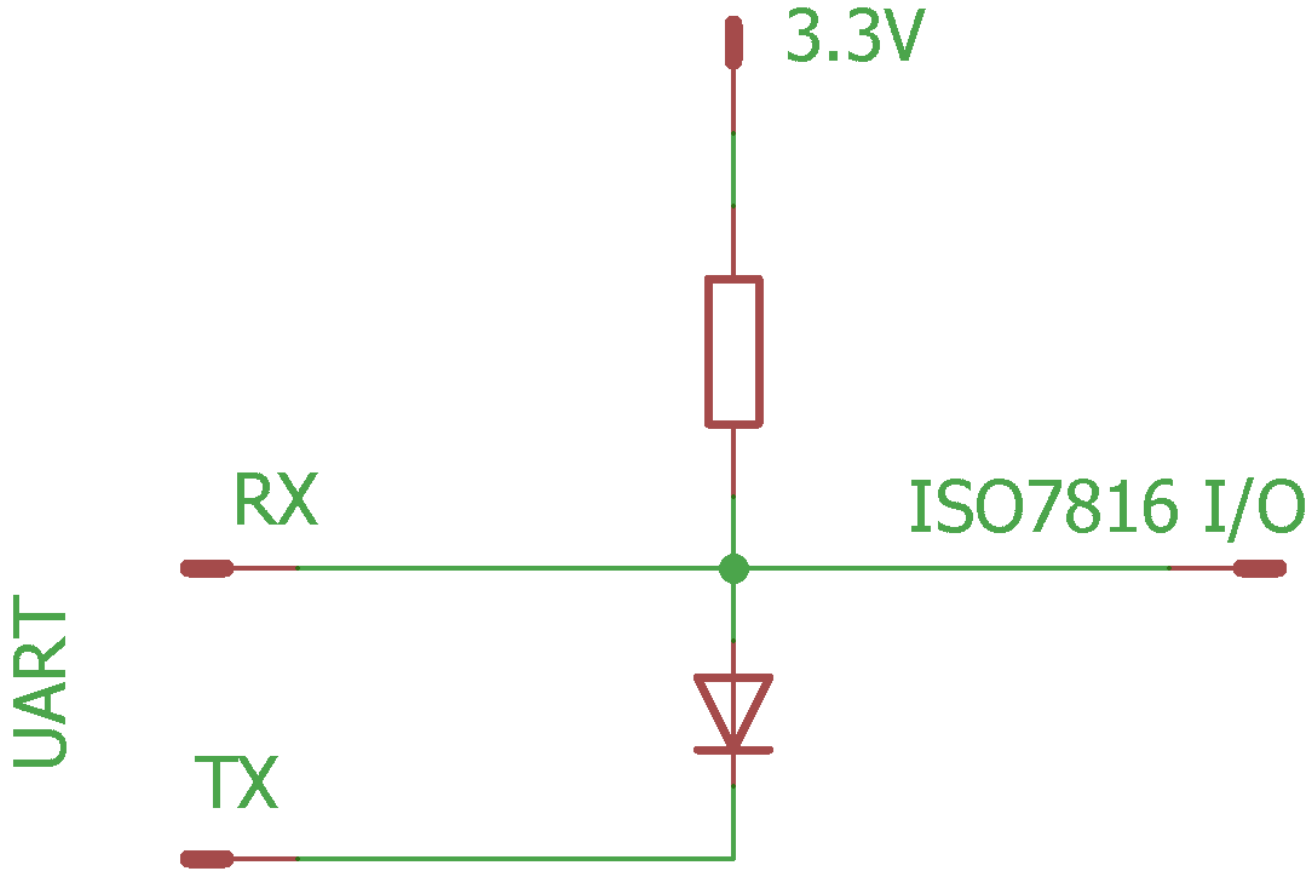
Implementácia: ISO7816
APDU (T=0)



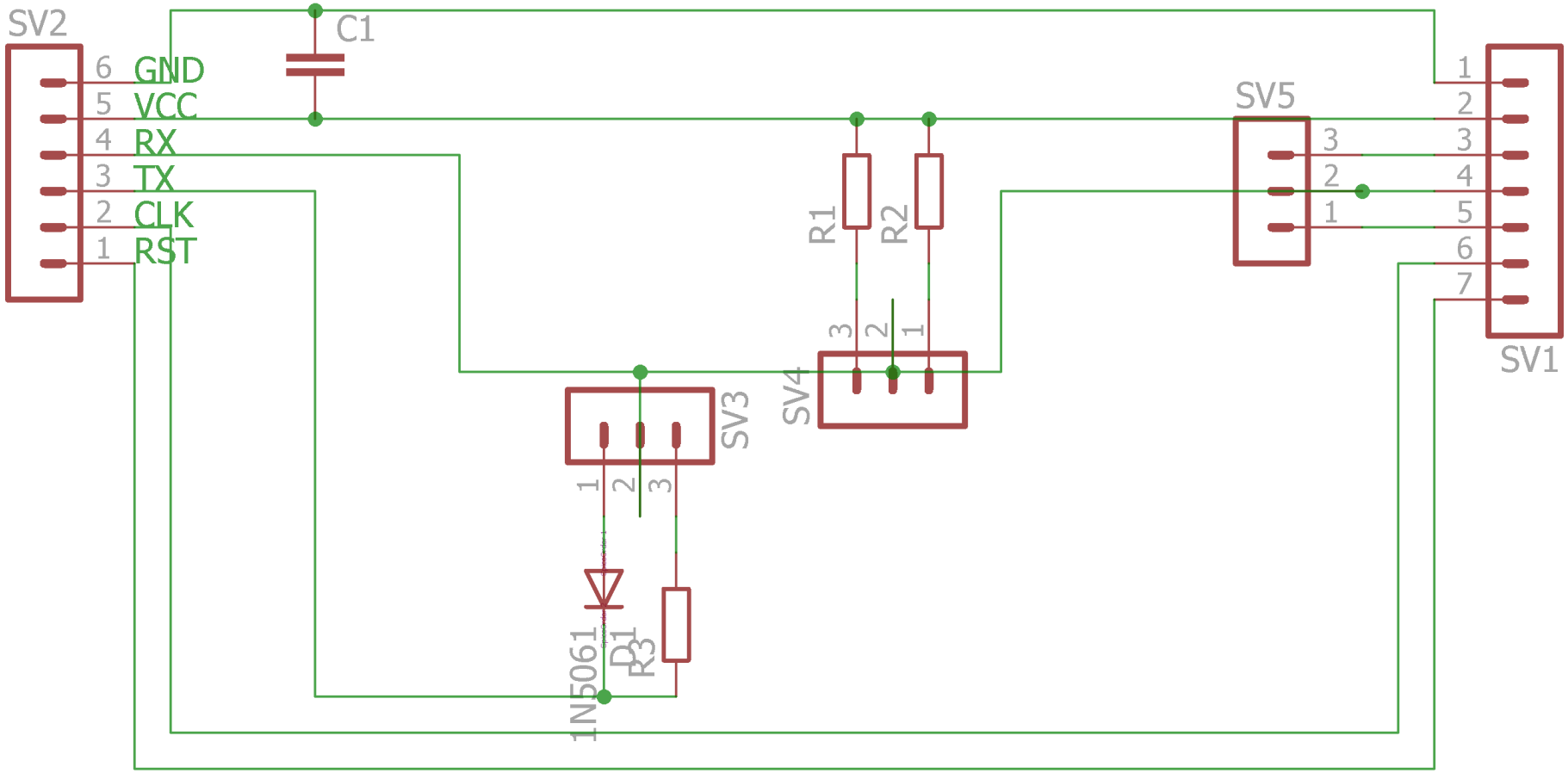
Implementácia: ISO7816
Blok dát (T=1)

Prologue Field			Information Field	Epilogue Field
Node Address NAD	Protocol Control Byte PCB	Length LEN	Optional INF	Error Detection LRC or CRC EDC
1 Byte	1 Byte	1 Byte	0-254 Bytes	1/2 Bytes

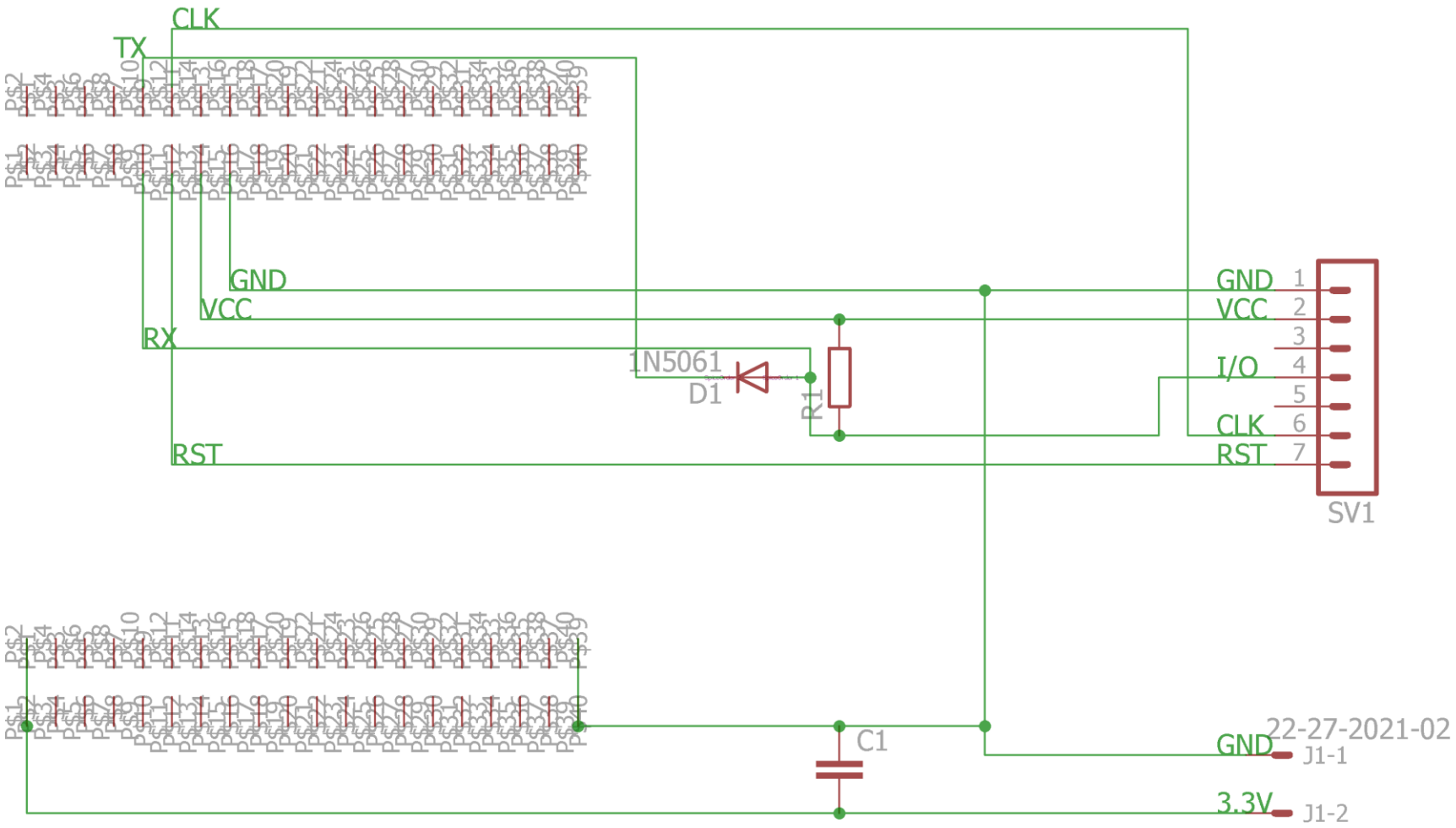
Implementácia-ISO7816 UART



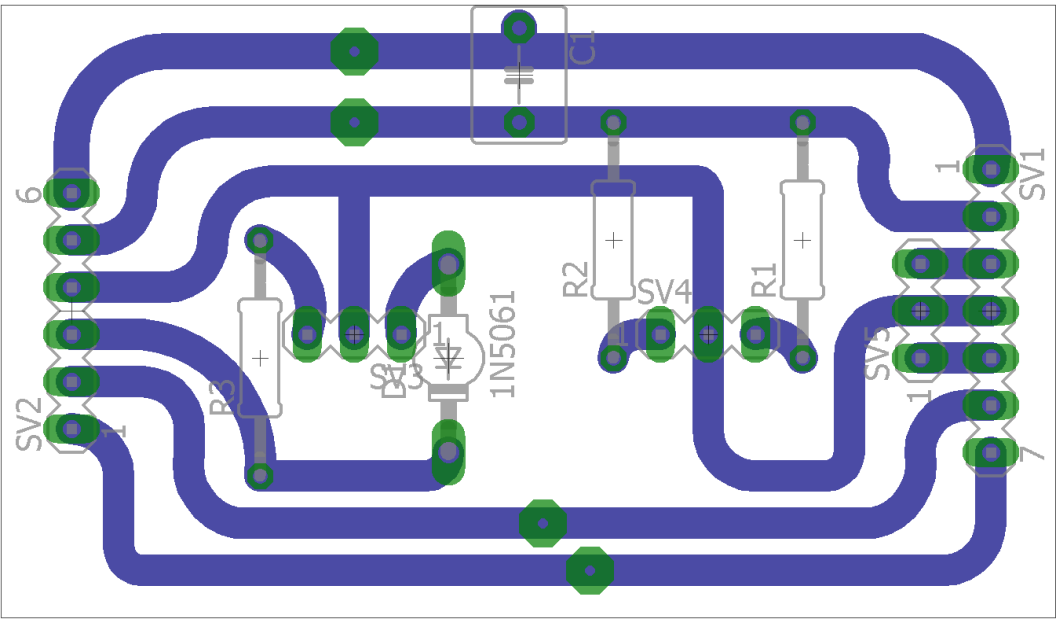
Implementácia: DPS I

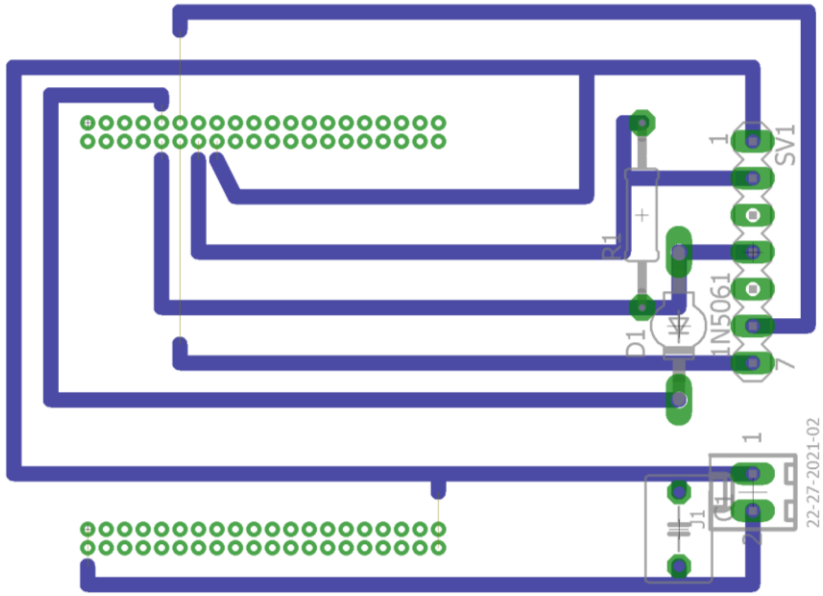


Implementácia: DPS II



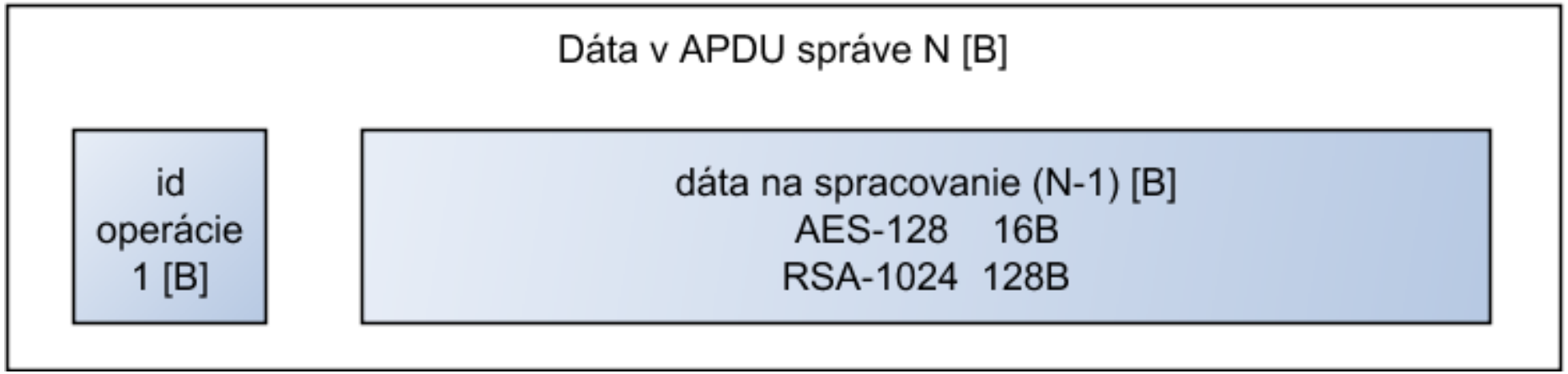
Implementácia: DPS





Implementácia: JC

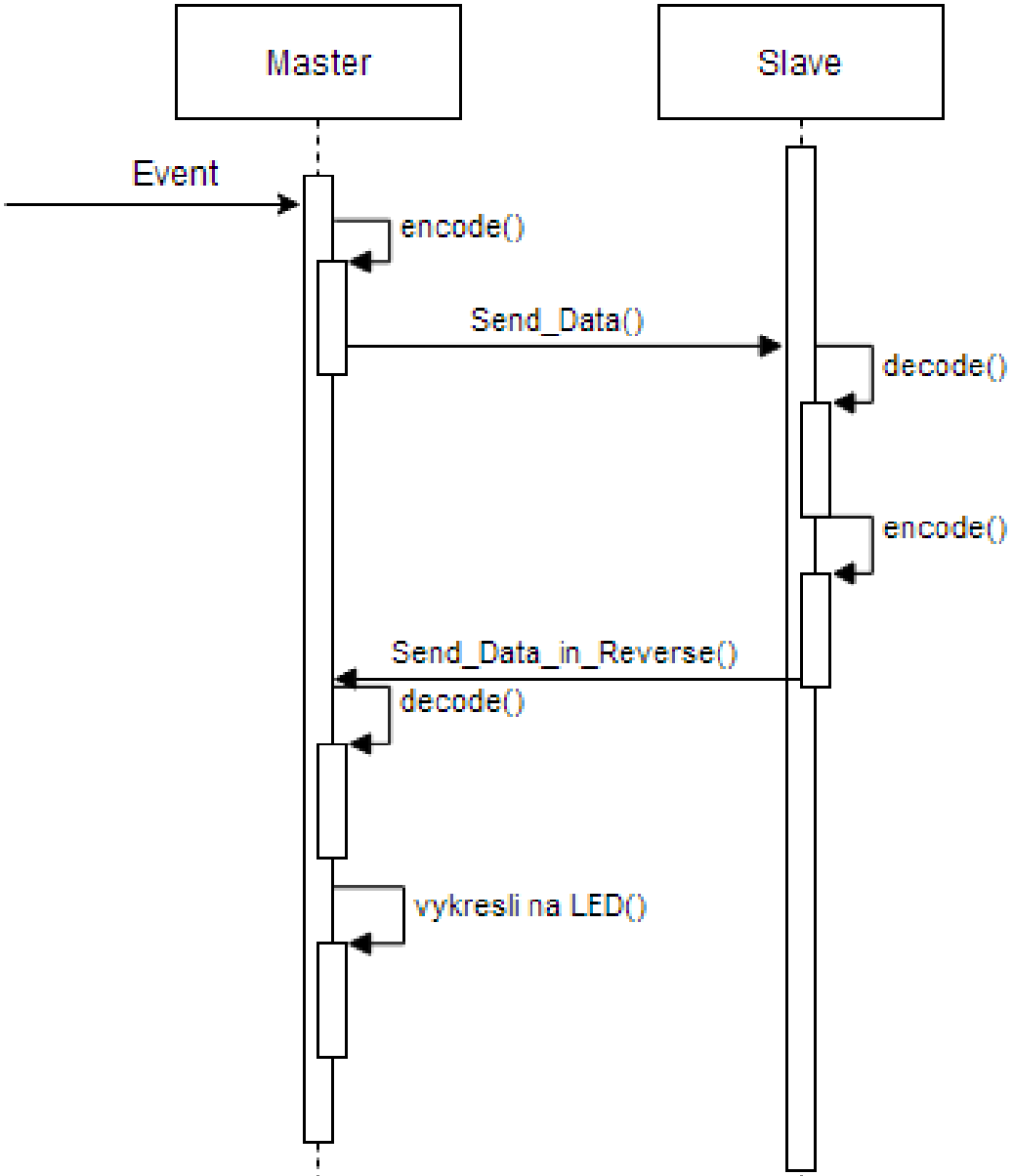
- Applet JC2.2.2
- HW AES-128 CBC
- APDU: Dáta
  - id operácie (enum), dáta



Implementácia: Konzola

- Segger J-Link RTT (Real Time Transfer)
  - monitorovanie, testovanie,
  - testovacie výpisy,
  - výpis ATR správy,
  - vyhľadávanie card manažéra,
  - posielanie APDU správy blokovo/bajtovo,
  - posielanie preddefinovaných správ,
  - aktivácia, deaktivácia, resetovanie,
  - prehľadávanie inštrukcií,
  - luďsky čitateľný výpis stavu z odpovedi,
  - zmenenie baudovej rýchlosti.

Testovanie


Master
Slave
Event
encode()
Send_Data()
decode()
encode()
Send_Data_in_Reverse()
decode()
vykresli na LED()

Vyhodnotenie testovania

Typ zabezpečenia	Metriky	
	Pamäť programu [B]	SRAM [B]
Žiadne zabezpečenie	7308	5696
SW AES 128 CBC	11336	6104
HW AES 128 CBC	18412	7960

Vyhodnotenie testovania

Typ zabezpečenia	Metriky
	Prúdová spotreba [mA]
Žiadne zabezpečenie	1.4
SW AES 128 CBC	5.6
HW AES 128 CBC	8

Vyhodnotenie testovania

Typ zabezpečenia	Metriky	
	Čas 200 [s]	Čas 1 interakcie [s]
Žiadne zabezpečenie	258.35	1.29175
SW AES 128 CBC	546.75	2.73375
HW AES 128 CBC	1638.47	8.19235

Vyhodnotenie testovania

Typ zabezpečenia	Metriky
	Network overhead [B]
Žiadne zabezpečenie	1x12
SW AES 128 CBC	3x12
HW AES 128 CBC	3x12

Sebakritika: čo sa nepodarilo

- RSA SW knižnice
- RSA HW (odhad)

Sebakritika: čo sa nefungovalo podľa predstáv

- Výsledky opačné, ako sa predpokladalo
  - v porovnaní s FPGA
  - GPIO, periférie, komunikácia, program, RAM
- postrácanie ANT paketov: po komunikácií s krypto-elementom

Záver

- Identifikované slabiny daných technológií so Smart kartami
- Na základe výsledkov sa dá spraviť odhad riešenia pomocou PKI

- Riešenie je vhodné:
  - reálnych aplikáciách (štandardizované, bezp.),
  - na rýchlejšie siete,
  - malé množstvo dát.

Plány do budúcna

- Spracovanie RF komunikácie pomocou udalostí:
  - Programová synchronizácia (*program, chyby*)

- overenia na iných komunikačných protokoloch,
- väčšiu sieť,
- testovanie zásobníka v neštandardných situáciach,
- testovanie, sniffer, Unit testy,
- Urýchlenie výpočtov/komunikácie s ISO7816:
  - vyššia rýchlosť CLK (*nábežné časy, šum*),
  - Secure messaging,
  - manuálny: select, upload, install (*reprogramovanie*).

Otázky

- Motivácia
- Informačná bezpečnosť
- Typy útokov
- Aktuálny stav vo WPAN 802.15
- Navrhnuté riešenie
- Implementácia
  - Komunikačný protokol
  - RF komunikácia
  - Segmentácia správ
  - SW AES-128 a HW AES-128
  - ISO7816, APDU, blok dát, UART
  - DPS
  - JavaCard
  - Konzola
- Testovanie a vyhodnotenie
- Sebakritika
  - Čo sa nepodarilo
  - Čo sa nefungovalo podľa predstáv
- Záver
- Plány do budúcna

Používané technológie

- Viac marketing ako technológie
  - iControl Networks: ZigBee, Z-Wave
  - BeeWi: Bluetooth
  - Samsung SmartThings hub: WiFi, Z-Wave, LAN, ZigBee

Odporúčané aplikácie sietí

- NFC
- RFID
- ANT
- Bluetooth
- ZigBee
- SigFox/LoRa WAN
- WiFi

- GSM

Veľkosť siete

Flexibilita

Spotreba

Kom. rýchlosť

Dosah

Prečo komunikačný protokol ANT?

- Nutné na niečom overiť riešenie, fyzické výsledky

- generické riešenie (roznorodosť)
- vždy bude nutnosť optimalizácie na HW

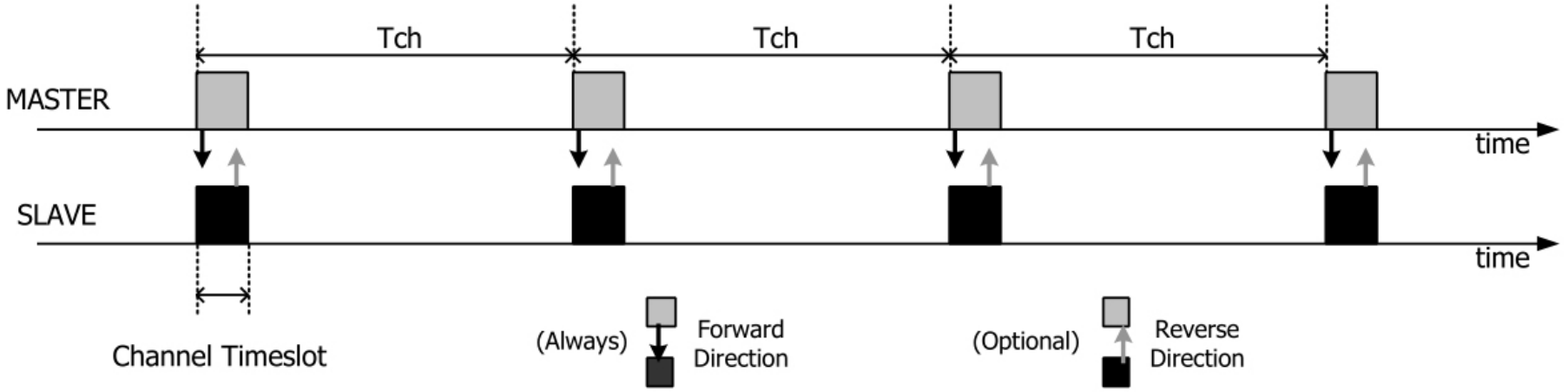
- bol po ruke

Najčastejšie dôvody porúch

- predpoklad že najmä kvôli
  - komunikácia s kryptoelementom (atomicky)
  - zmeškanie časového okna pre posielanie: rozsynchronizovanie protokolu

- Protiopatrenia
  - predpripravovanie dát, posielanie neskôr
  - SoftDevice: kontrola, či sa nič neposiela

Najčastejšie dôvody porúch



Ako urýchliť HW kryptovanie?

- vyššia rýchlosť ext. CLK pomocou GPIO
- dedikovaný periférie pre ISO7816 (atmel)
- konverter na ISO7816

- bude to niečo stáť
  - vývoj,
  - narastie veľkosť programu,
  - možnosť výskytu chýb.