

Zabezpečenie bezdrôtových komunikačných sietí v inteligentných domácnostiach proti kybernetickým útokom

Bc. Lukáš Doubravský

14. 06. 2017

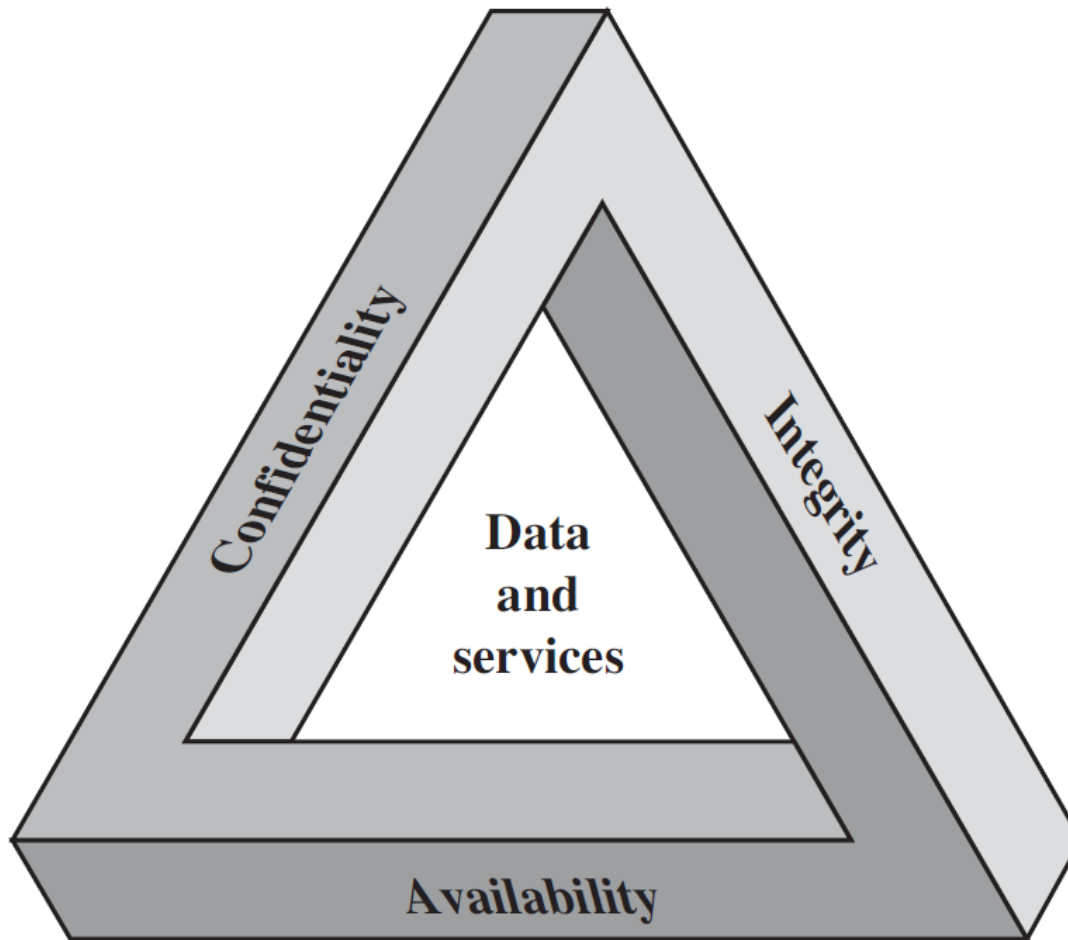
Motivácia

- bezpečnosť je neustály boj,
- verzie kryptografických algoritmov,
- tam, kde pred tým nebola,
- efektívnejšie,
 - pamäť,
 - spotreba,
 - rýchlosť.

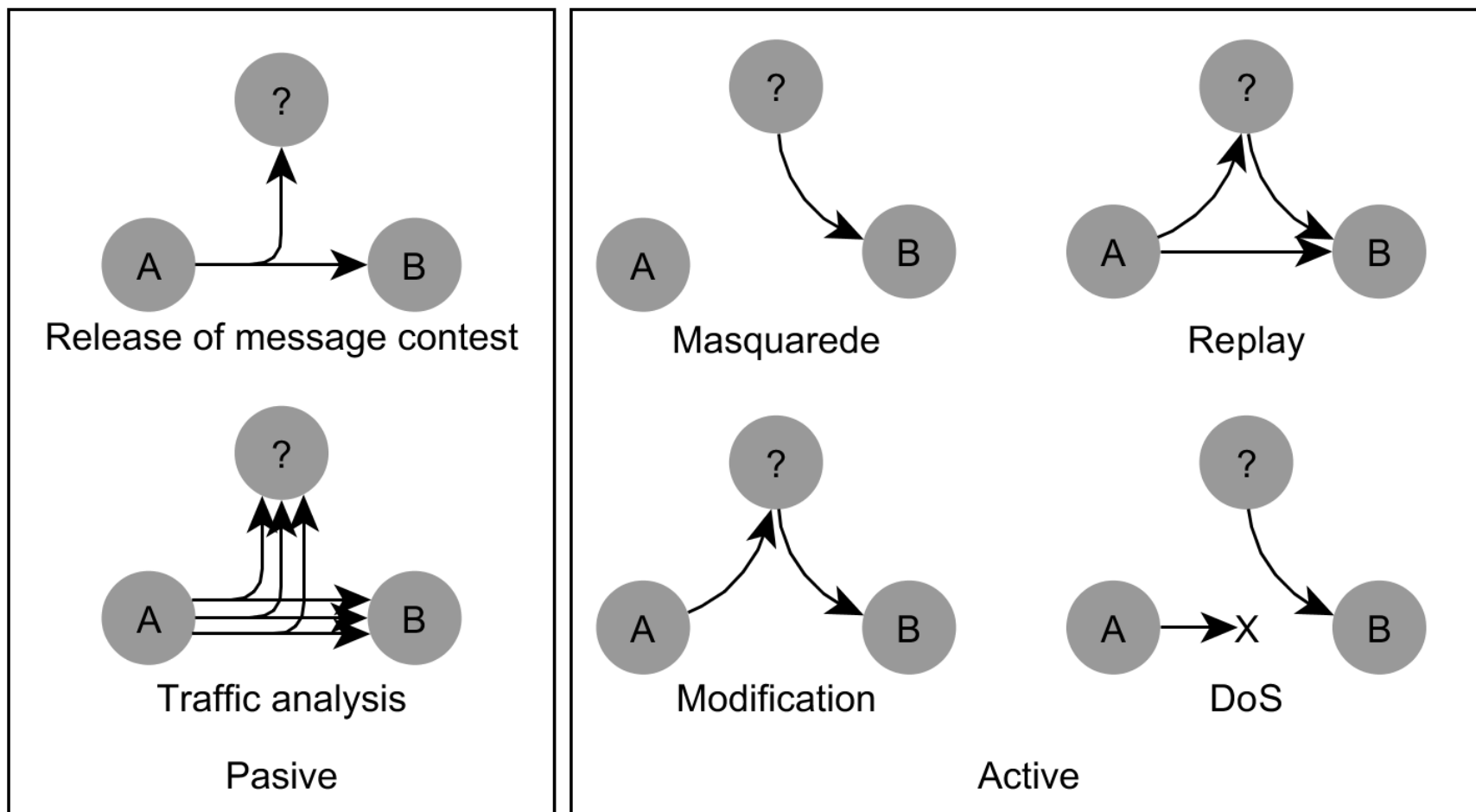
Cieľ

- Zvýšiť zabezpečenie v bezdrôtových komunikačných sieťach v inteligentných domácnostiach

Informačná bezpečnosť



Typy útokov



Aktuálny stav vo WPAN 802.15

- Zabezpečenie hlavne na transportnej vrstve
- ANT: AES-128
- Bluetooth: AES-CMAC (128)
- ZigBee: AES-128
- LoRaWAN: AES-128

Navrhnuté riešenie

- Použitie hardvérových kryptografických algoritmov
 - každý senzor osadený kryptoelement.
- Zabezpečiť komunikáciu medzi:
 - senzorom,
 - najbližším zariadením s výpočtovým výkonom (cloud, HUB).

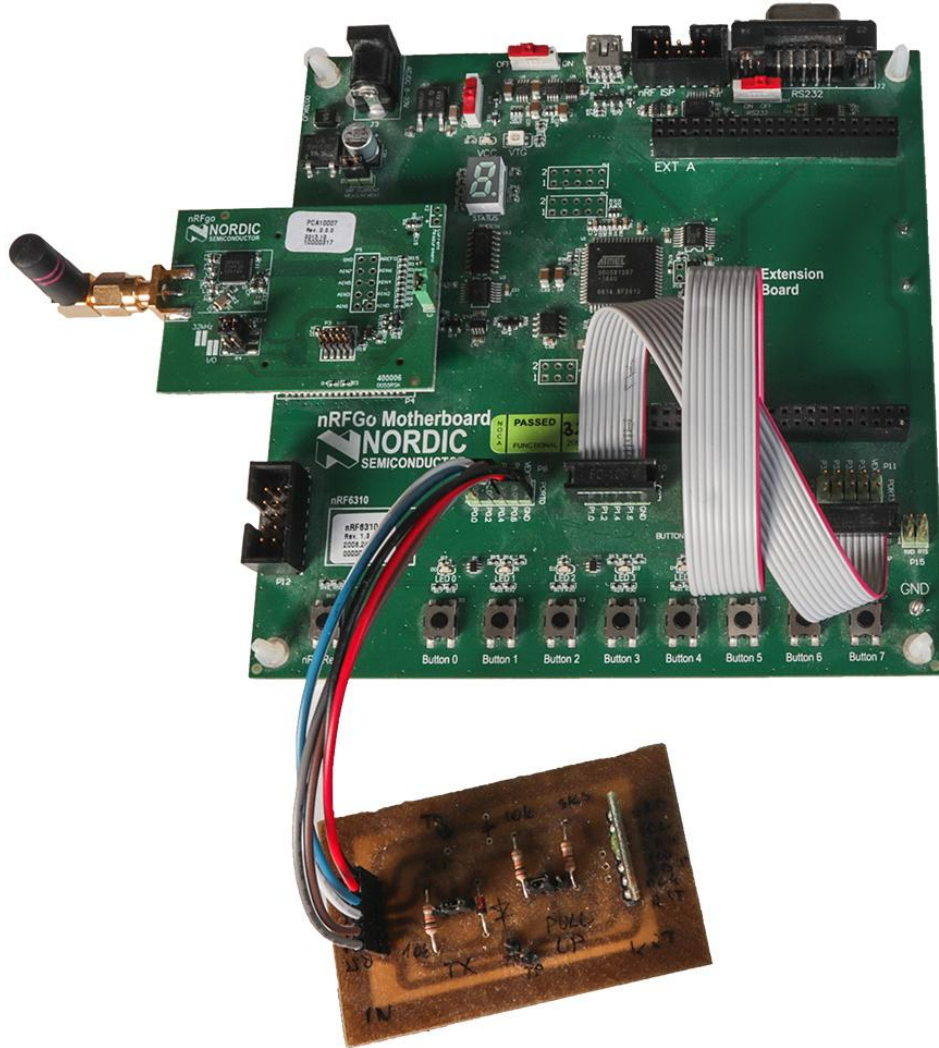
Navrhnuté riešenie

- centralizovaná architektúra siete,
- PKI
 - RSA/ECC-AES + podpisové schémy
 - certifikáty (obmedzenej forme)
- Autentifikáciu na aplikačnej vrstve
 - ostatné aspekty inf. bezp. sa dajú zabezpečiť nad touto vrstvou
- Overenie na rovnakej architektúre:
 - nezabezpečená komunikačná sieť
 - SW a HW zabezpečenie

Implementácia: Bezdrôtová komunikácia

- Nordic Semiconductors (nRF51422)
 - C,
 - ANT SoftDevice, 2.4 GHz,
 - ARM, 32bit architektúra,
 - 256 kB program, 16kB RAM.

Implementácia: Model siete



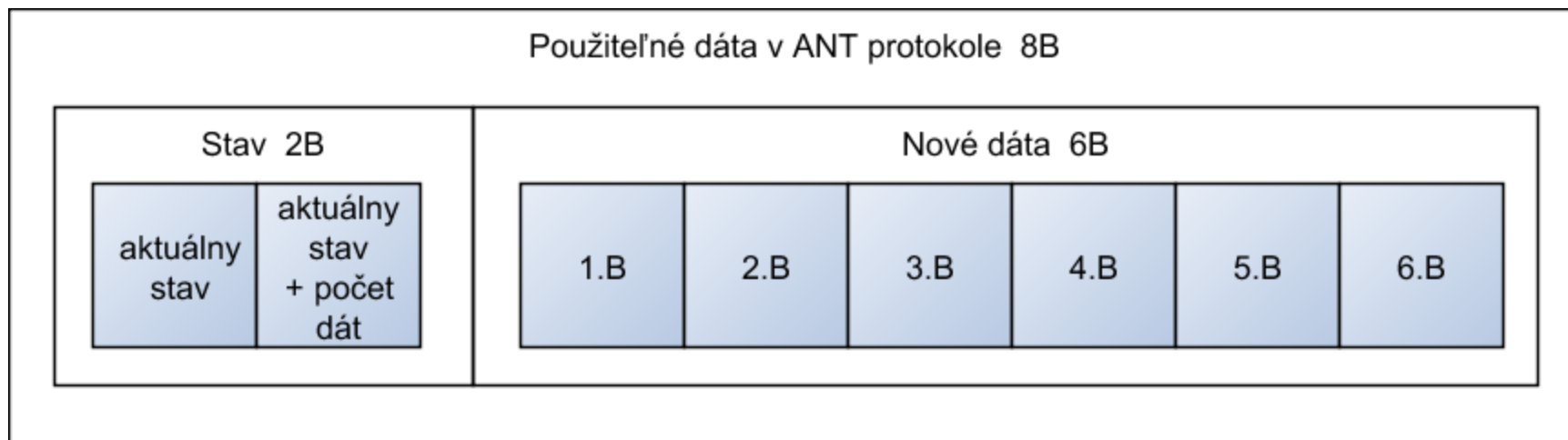
"Master" kontakt s prostredím



"Slave"

Implementácia: Segmentácia správ

- Viac ako 8 bajtov, maximálne 254 bajtov



- Príklad správ

– 00 00 ...

prázdna správa

– 01 03 01 FF ...

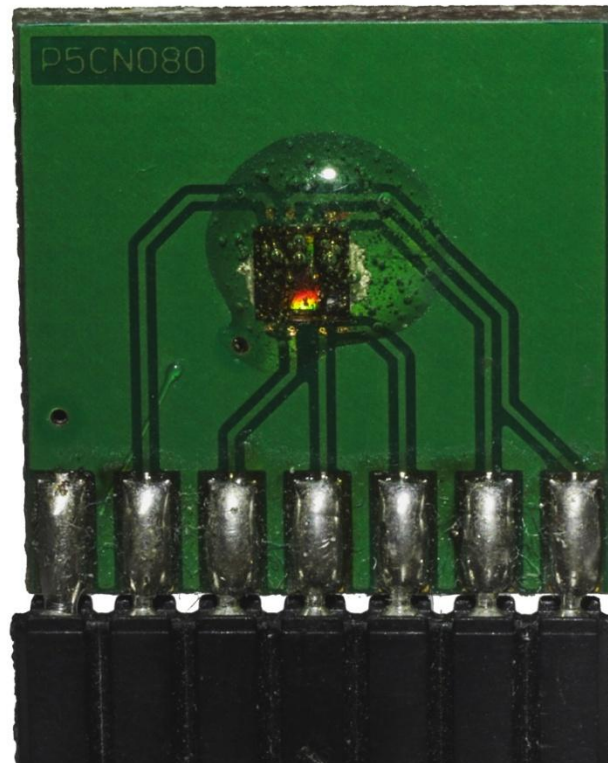
nezabezpečená správa

Implementácia: SW AES

- referenčná SW implementácia pre zabezpečenie komunikačného kanála
- knižnica: Tiny AES128 v jazyku C
- mód: CBC

Implementácia: HW AES

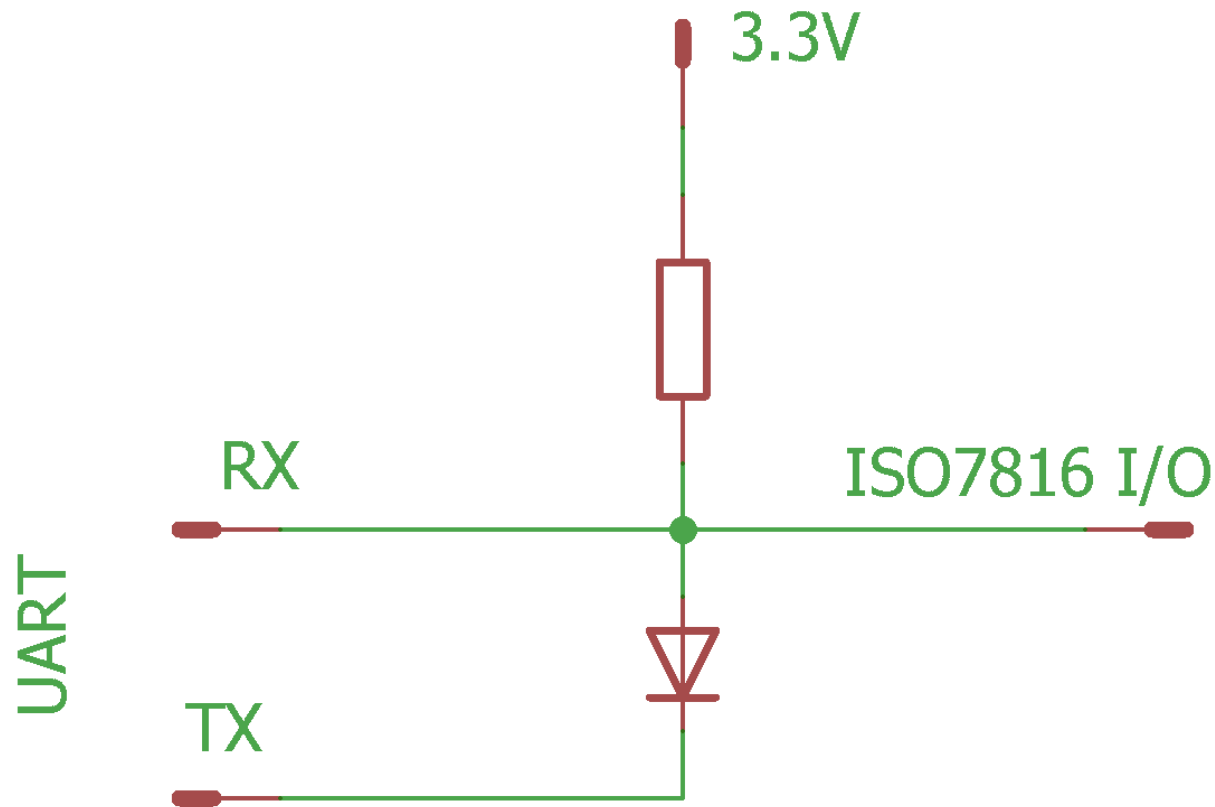
- NXP, Secure element, JVM
- HW: NFC, RNG, RSA, ECC, AES, DES koprocessor apod.



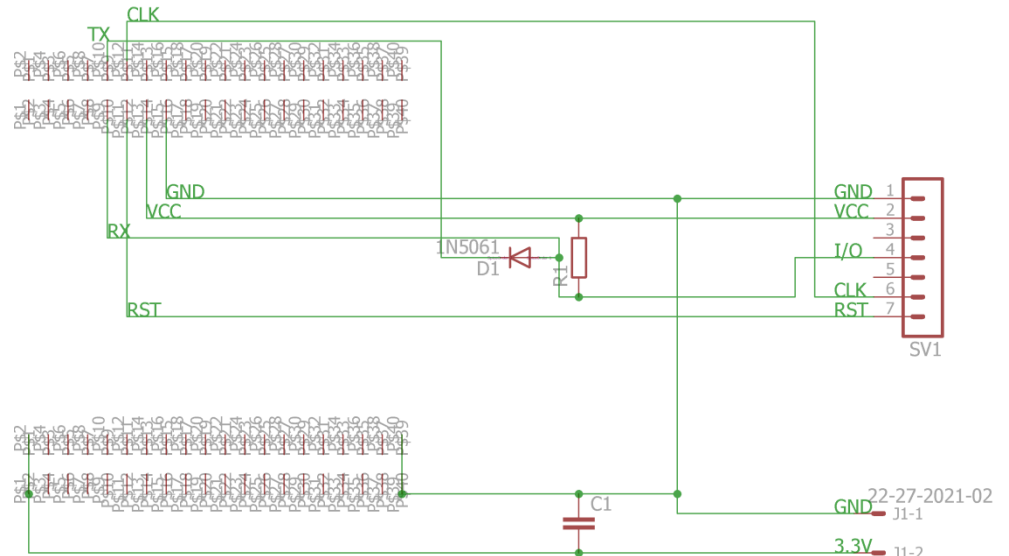
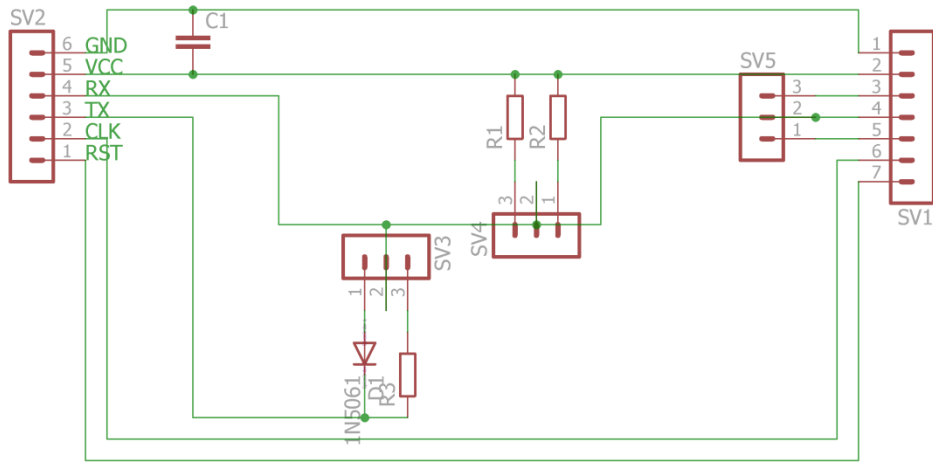
Implementácia: ISO7816

- pre kontaktné Smart karty
 - SIM,
 - platobné karty.
- signály sú generované SW: GPIO a HW periférií (*PPI*)
 - CLK: 2.667 MHz.
- ISO7816 I/O signál na UART
 - Baud rate: 7168 bps
- ATR (answer to reset), informácie o karte, preferované nastavenia
- Komunikácia:
 - T=0 bajtová: APDU
 - T=1 bloková: APDU zabalené do bloku

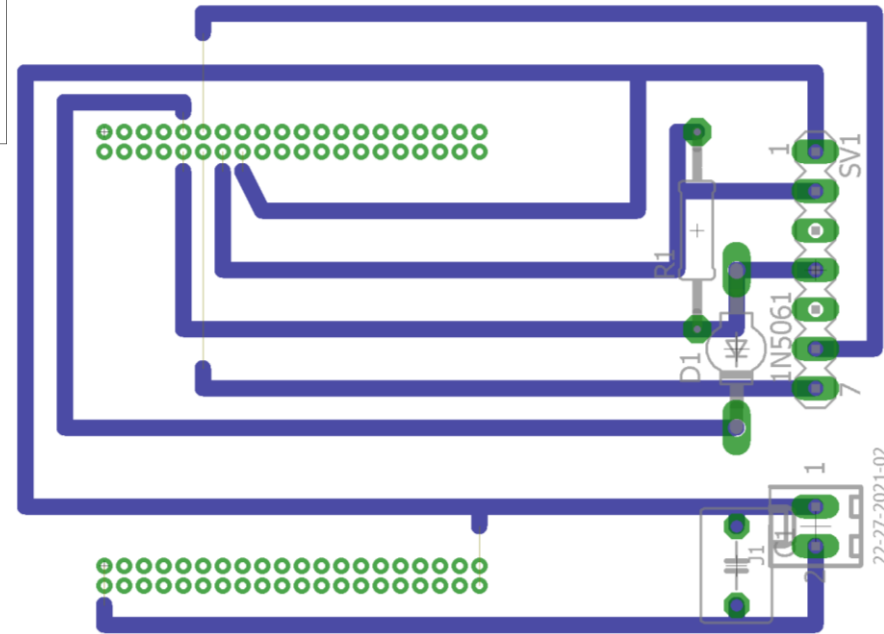
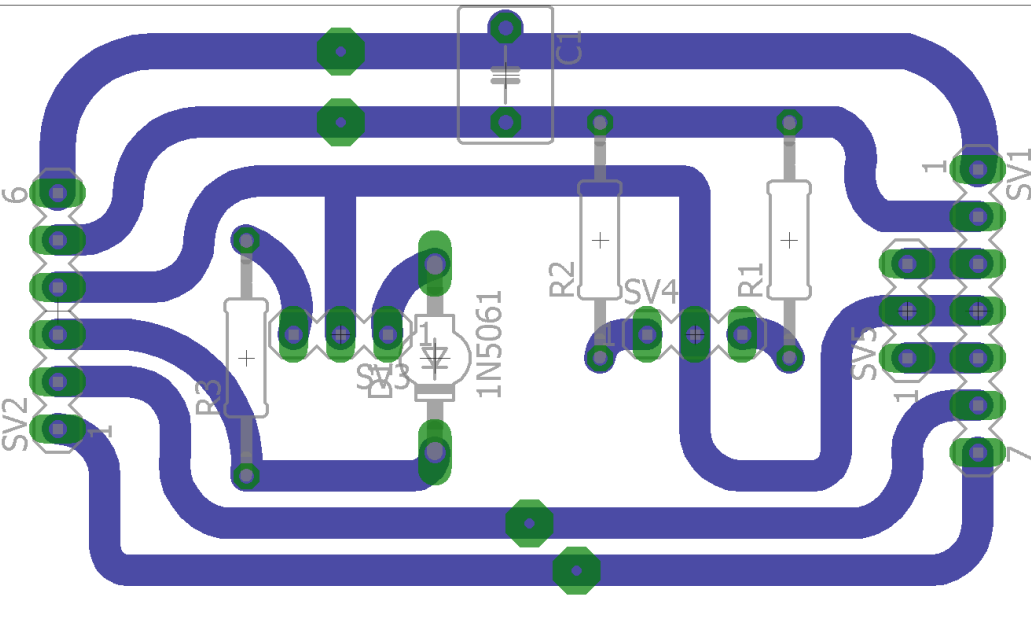
Implementação: ISO7816 na UART



Implementácia: Schémy

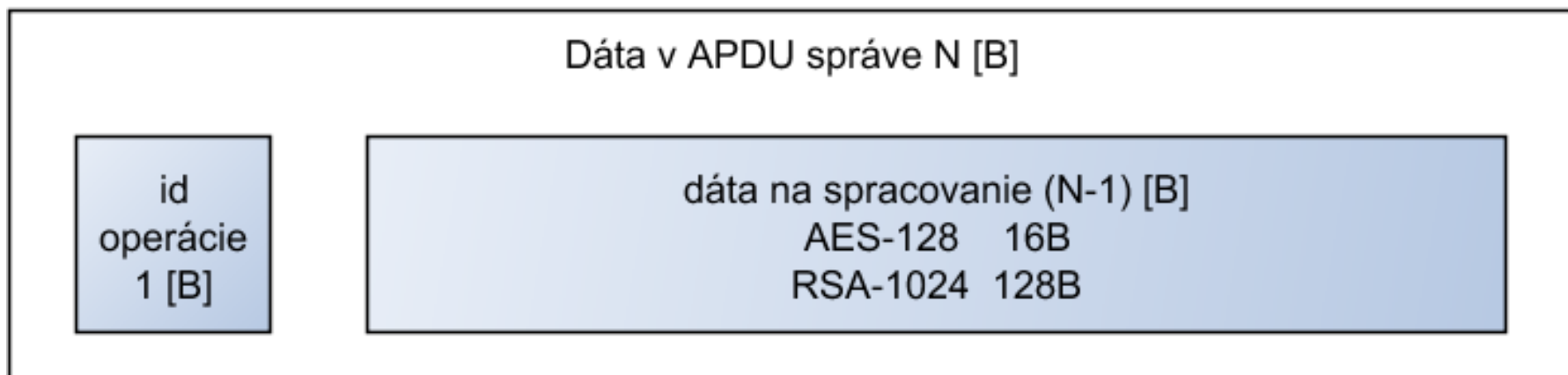


Implementácia: DPS



Implementácia: JavaCard

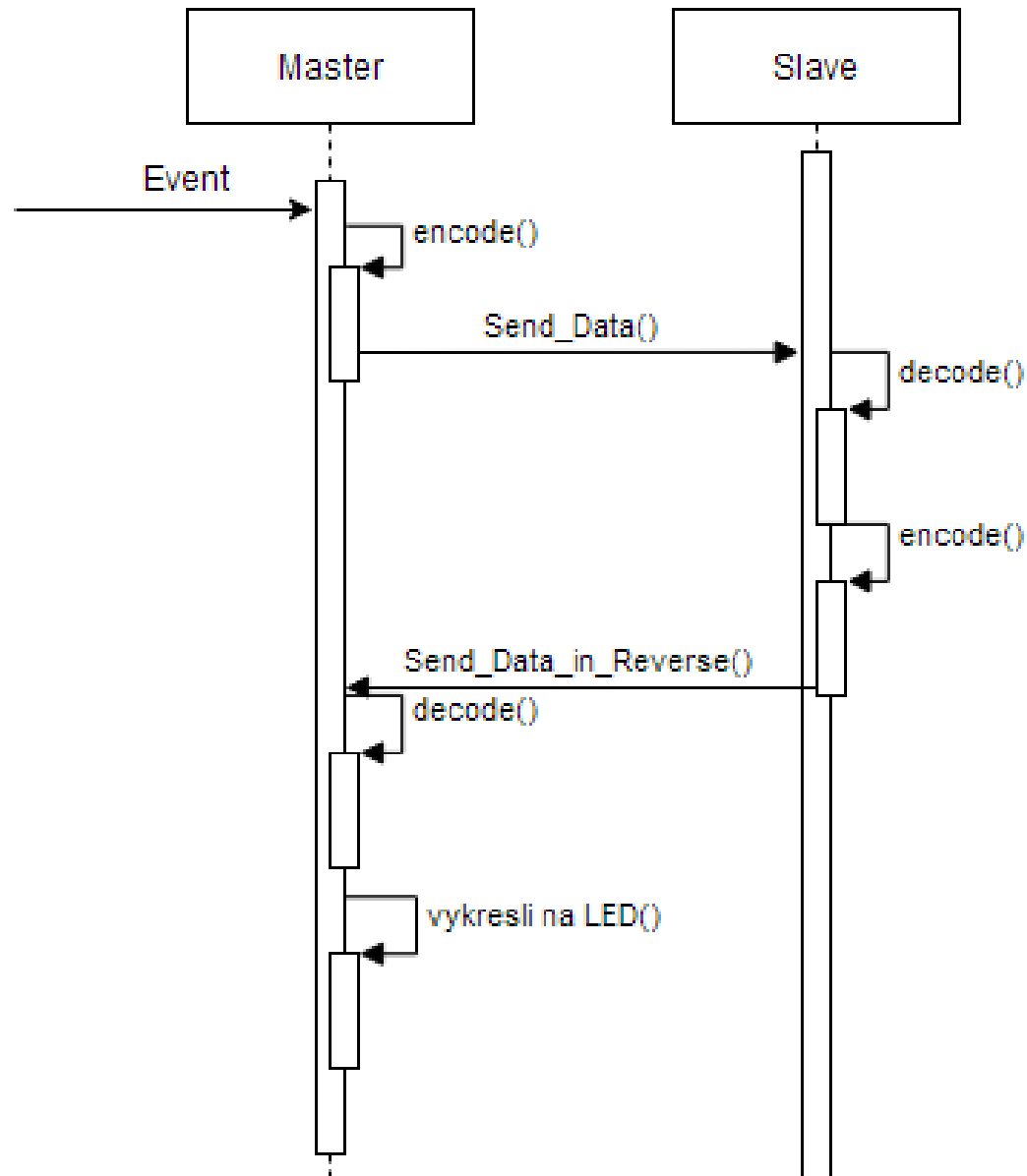
- Applet JC2.2.2
 - Java
- hardvérovo impl. alg. AES-128 CBC
- formát správy APDU (terminál-SmartCard)



Implementácia: Funkc. konzoly

- desktop-senzor,
- Segger J-Link RTT (Real Time Transfer):
 - monitorovanie,
 - testovanie ISO7816,
 - posielanie APDU správy blokovo/bajtovo,
 - vyhľadávanie manažéra karty,
 - ľudsky čitateľný výpis stavu z odpovedi.

Testovanie



Výsledky testovania

| Typ zabezpečenia | Metrika | |
|-----------------------|--------------------|----------|
| | Pamäť programu [B] | SRAM [B] |
| Nezabezpečený kom. | 7308 | 5696 |
| SW AES 128 CBC | 11336 | 6104 |
| HW AES 128 CBC | 18412 | 7960 |

- Nárast veľkosti programu, a to aj pri HW zabezpečení

Výsledky testovania

| Typ zabezpečenia | Metrika |
|-----------------------|-----------------------|
| | Prúdová spotreba [mA] |
| Nezabezpečený kom. | 1.4 |
| SW AES 128 CBC | 5.6 |
| HW AES 128 CBC | 8 |

- Nárast prúdovej spotreby, aj pri HW zabezpečení

Výsledky testovania

| Typ zabezpečenia | Metrika | |
|-----------------------|------------------------|----------------------|
| | Čas 200 interakcií [s] | Čas 1 interakcie [s] |
| Nezabezpečený kom. | 258.35 (4 min.) | 1.29175 |
| SW AES 128 CBC | 546.75 (9 min.) | 2.73375 |
| HW AES 128 CBC | 1638.47 (27 min.) | 8.19235 |

- Dĺžka vykonania testu, aj pri HW zabezpečení

Vyhodnotenie

- Prekvapený výsledkami HW riešenia, (opačné ako sa predpokladalo)
 - veľkosť programu: štandard ISO7816,
 - spotreba: aktivované viaceré periférie,
 - čas komunikácie: protokolový zásobník, strata paketov.
- PKI
 - RSA SW knižnice v C

Záver

- nepodarilo sa zvýšiť zabezpečenie,
 - na základe výsledkov sa dá spraviť odhad riešenia pomocou PKI.
- PKI by bolo možné, riešenie by bolo použiteľné:
 - na rýchlejších sieťach,
 - malé množstvo dát (ISO7816).

Plány do budúcnosti

- spracovanie bezdrôtovej komunikácie pomocou udalostí:
 - programová synchronizácia (*program, chyby*)
- overenia na iných komunikačných protokoloch,
- väčšiu sieť,
- PKI,
- urýchlenie výpočtov/komunikácie s ISO7816:
 - Secure channel a manuálnu inštaláciu appletu.

Otázky?

- Motivácia
- Informačná bezpečnosť
- Typy útokov
- Aktuálny stav vo WPAN 802.15
- Navrhnuté riešenie
- Implementácia:
 - Bezdrôtová komunikácia
 - Model siete
 - Segmentácia správ
 - SW AES-128 a HW AES-128
 - ISO7816
 - Schémy, DPS
 - JavaCard
 - Funkcionalita konzoly
- Testovanie a vyhodnotenie
- Sebakritika
- Záver
- Plány do budúcnosti

Používané technológie

- Viac marketing ako technológie a parametre:
 - 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

Parametre:

Veľkosť siete

Flexibilita

Spotreba

Kom. rýchlosť

Dosah



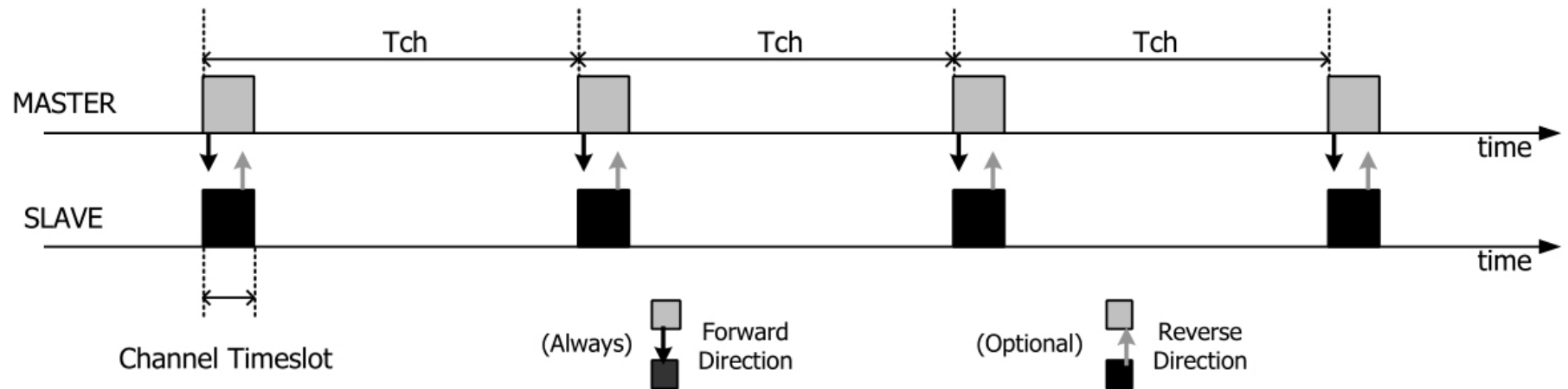
Prečo komunikačný protokol ANT?

- nutné na niečom overiť riešenie a získať fyzické výsledky,
- generický návrh (rôznorodosť),
- IoT, WSN, vždy bude nutnosť optimalizácie na HW
- bol dostupný

Najčastejšie dôvody porúch

- Protiopatrenia:
 - pred-pripravovanie dát, posielanie neskôr,
 - SoftDevice: kontrola, či sa niečo posiela.
- Predpoklad (bez podrobného testovania):
 - komunikácia s kryptoelementom (atomicky),
 - zmeškanie časového okna pre posielanie:
rozsynchronizovanie protokolu.

Najčastejšie dôvody porúch

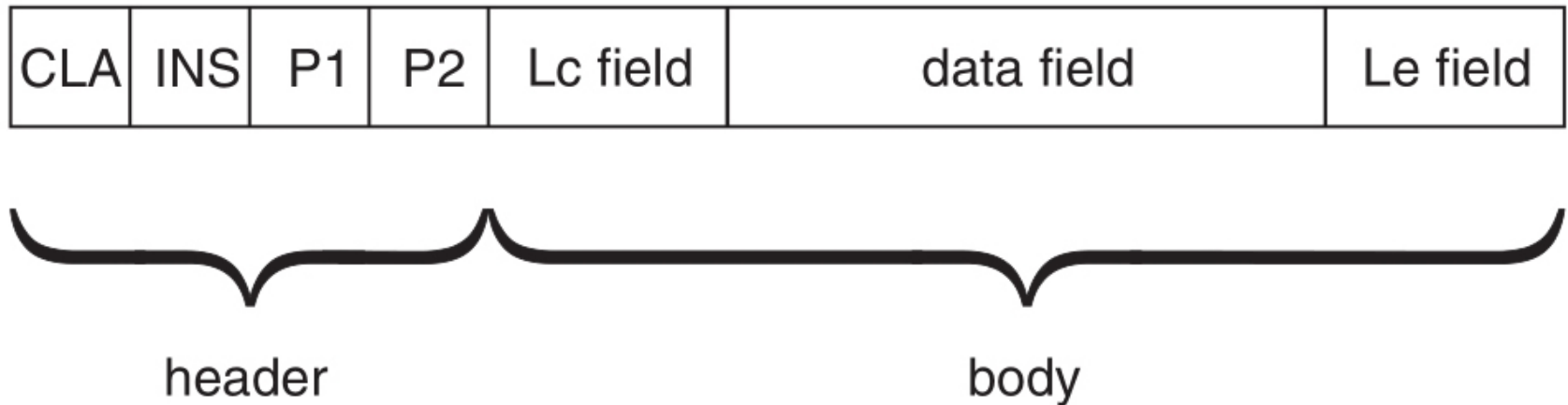


Zefektívnenie HW kryptovania

- Predpripraviť dáta vo vhodný okamich, programovú synchronizáciu,
- vyššia rýchlosť ext. CLK pomocou GPIO,
 - programovo max. 4MHz s 16MHz kryštálom
 - dedikovaný oscilátor max. 20MHz pri niektorých smart kartách
- dedikované periférie pre ISO7816 (atmel),
- konvertor na ISO7816.
- môže narásť:
 - veľkosť programu,
 - cena a čas vývoja,
 - možnosť výskytu chýb a porúch.

Implementácia: ISO7816

APDU (T=0)

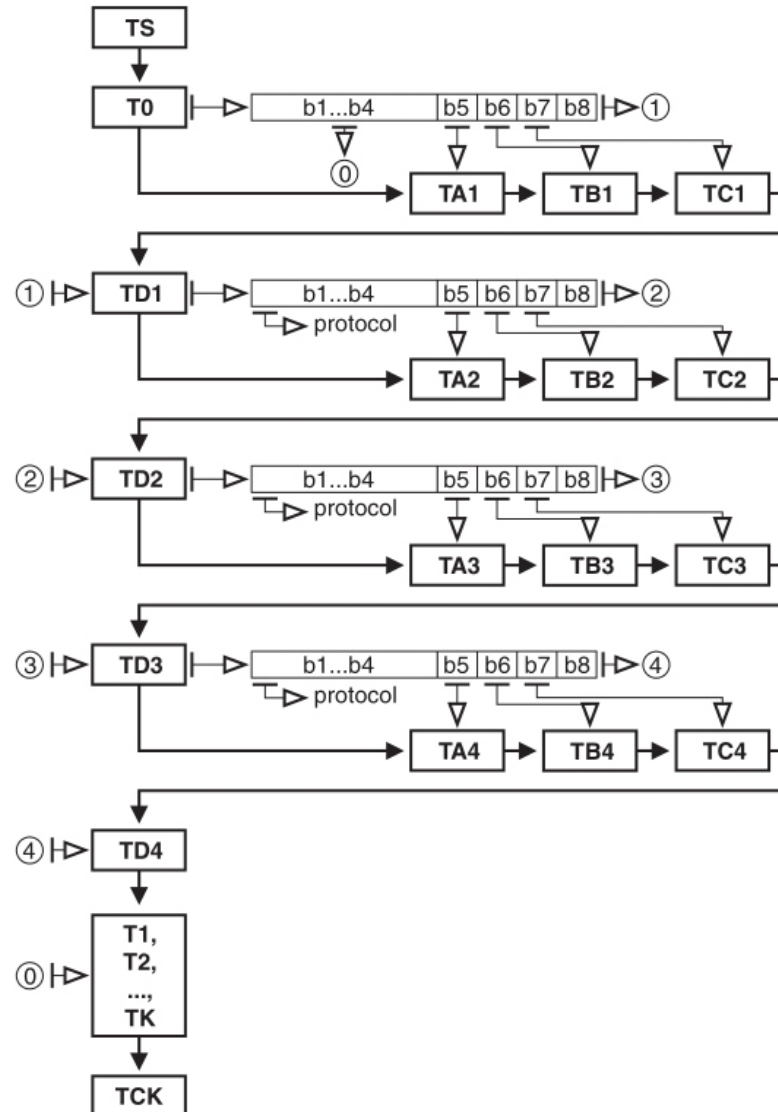


Implementácia: ISO7816

Blok dát (T=1)

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

Implementácia: ISO7816 ATR



Výsledky testovania

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

- $(1B + 16B) / 6B = 3$ pakety