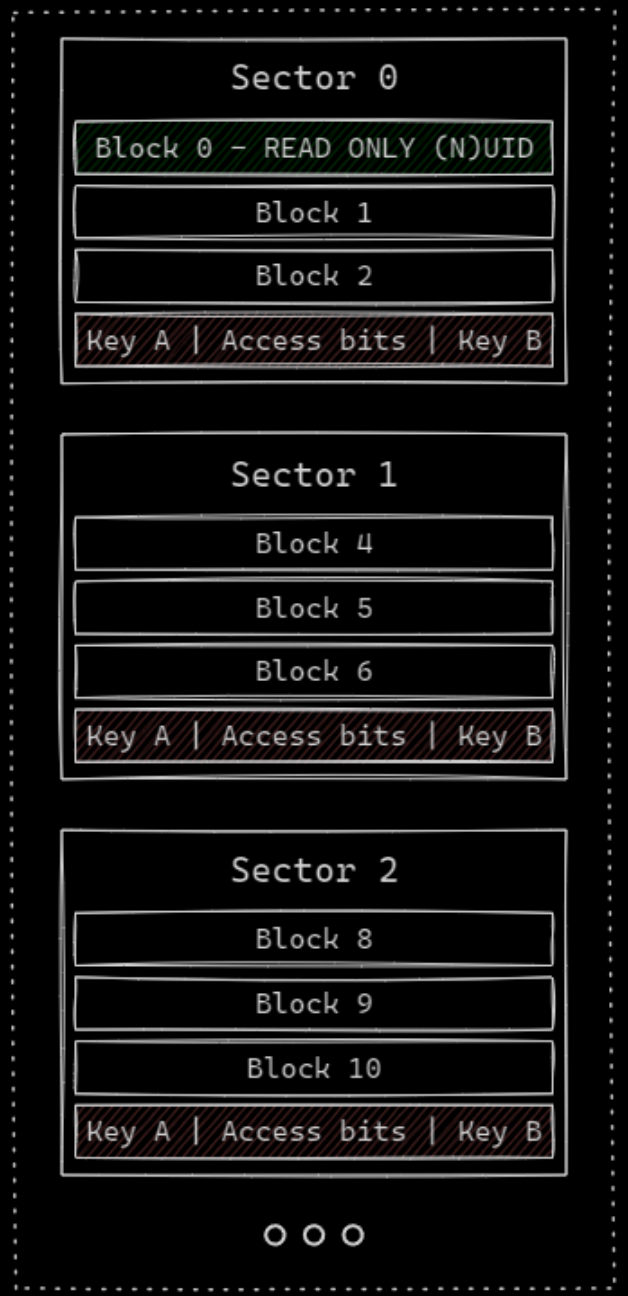
Attendance monitoring system

By Božo Durdov & Duje Glavina

Table of contents

RFID tag crash course

- RFID 13.56 Mhz read/write ISO-14443A tag



1. Current solutions and issues

Current solutions

PMF / SVK

- Standard UID-based access control

```
Sector: 0

CFDDA10FBC38020000000000021074400
00011D581E581F58295800000000000000
00000000000000000000000000000000
A0A1A2A3A4A5787788C2------------
```

FESB / SVK

- The access key is stored in reader

```
Sector: 1

60198321002313870650000023138706
32303233313030313901140315706D00
32330000000000060030325352434504
21F5A3C93807787788 00------------
```

Issues

PMF / SVK

- Security: UID is set in factory and cannot be altered. Only vendor knows how to make a tag.
- Magic cards
- Emulators

FESB / SVK

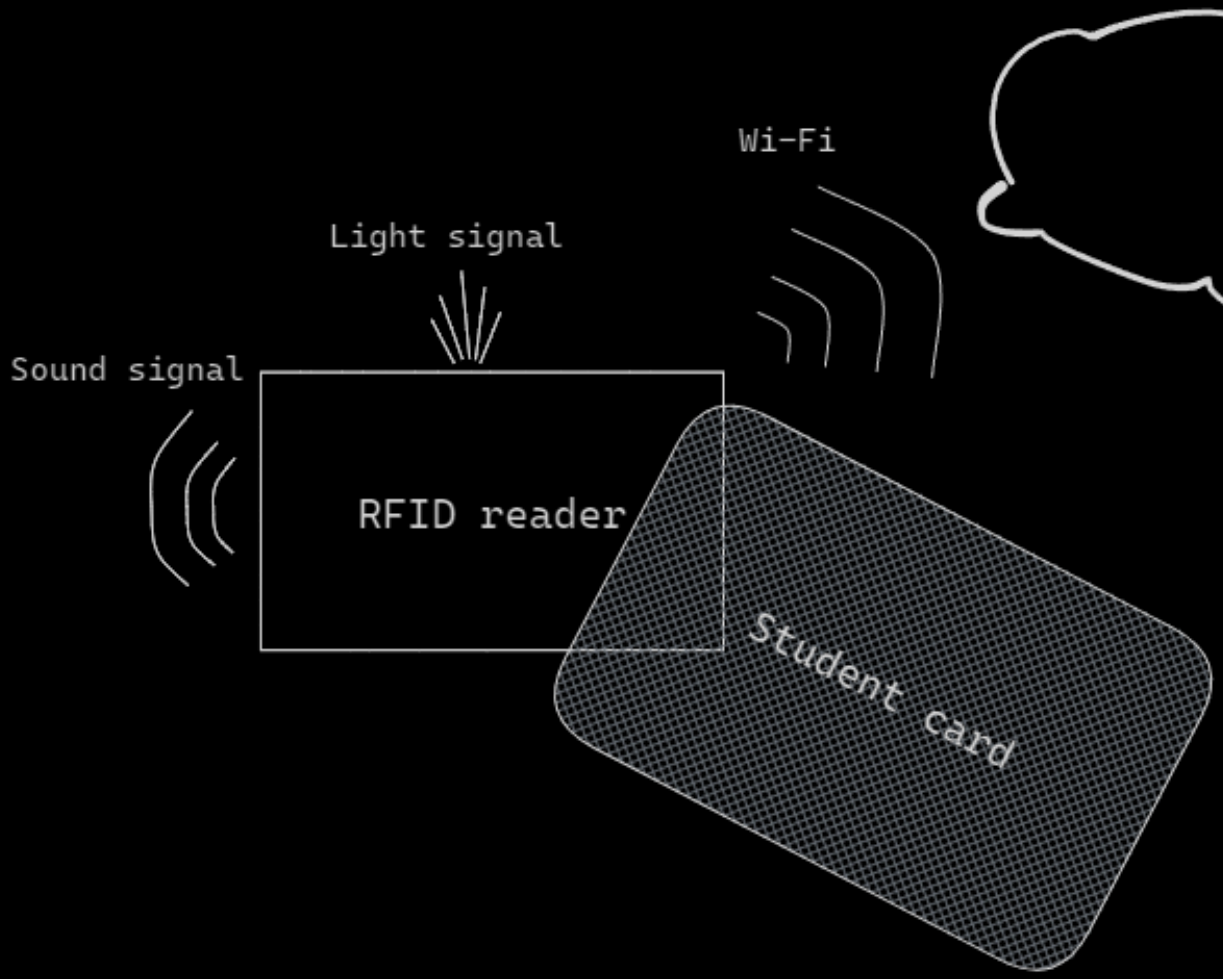
- Security: *Only valid reader can access the data stored on card*
- *„Break a single reader once and enter anywhere”*

Milosch Meriac, 2010

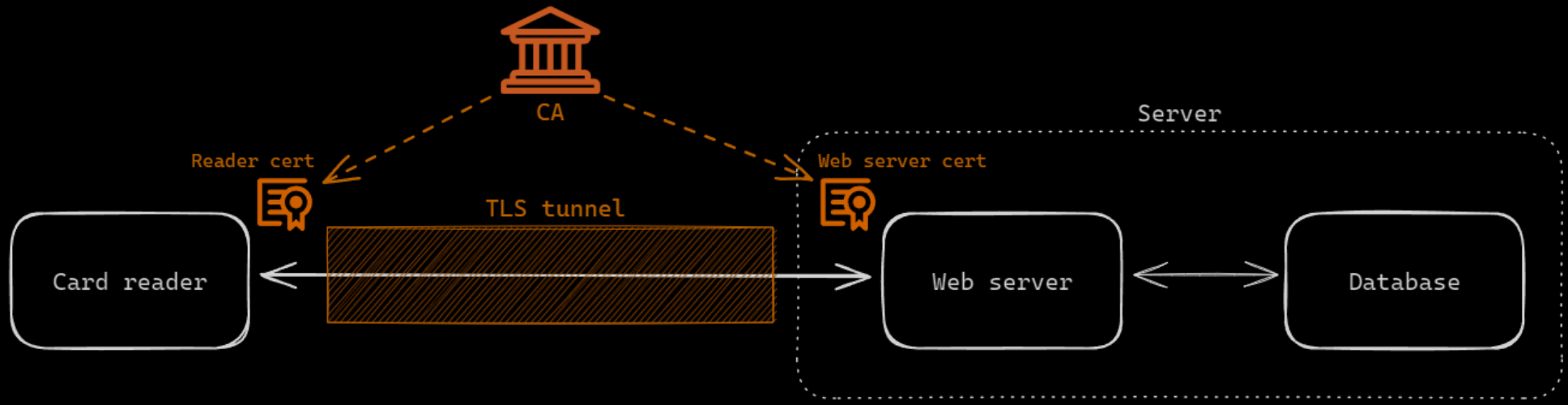
Test FESB / SVK

- ✓ Recording student attendance
- ✓ Enter library

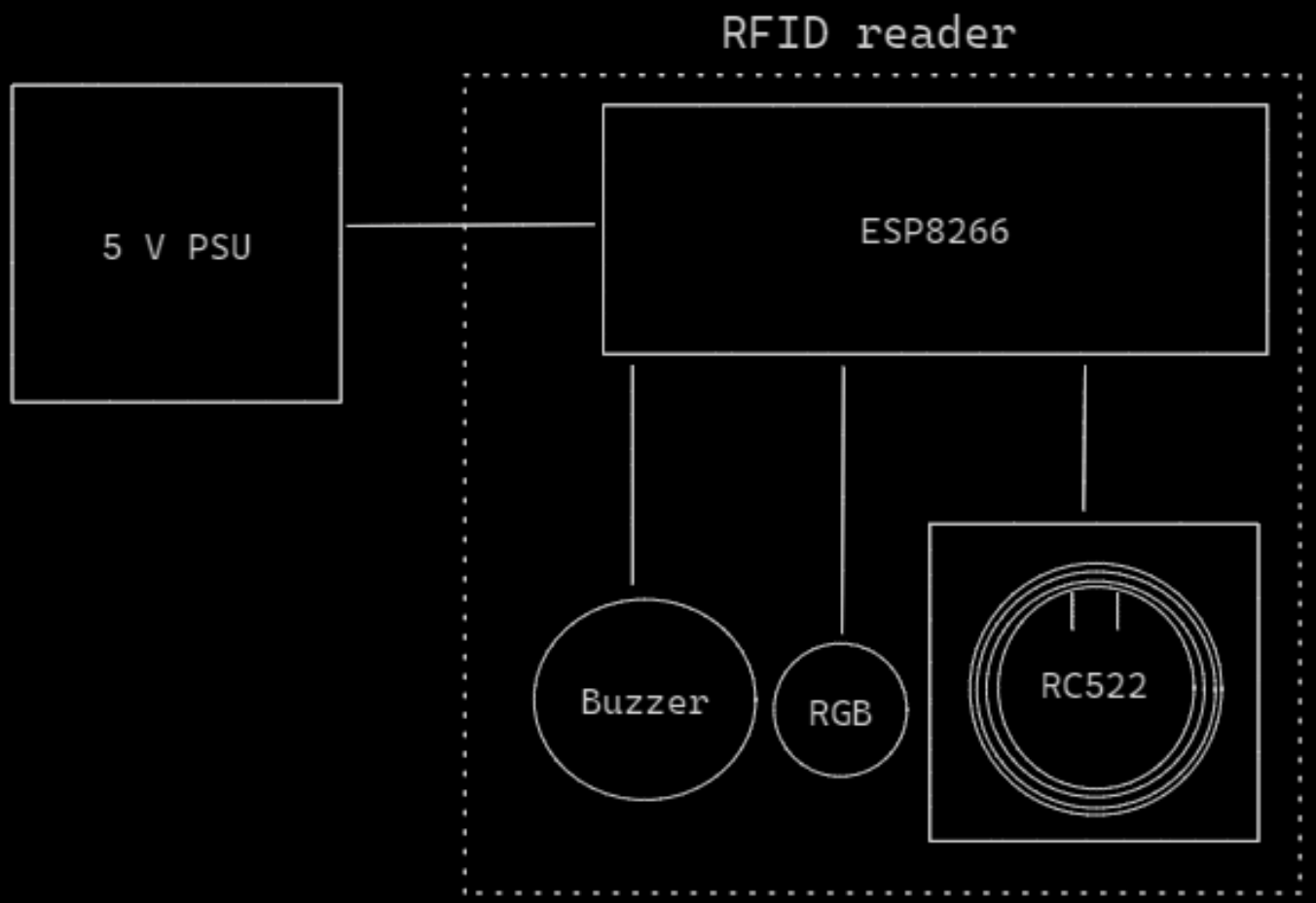
Solution proposal



- Master key
- Each card has unique key

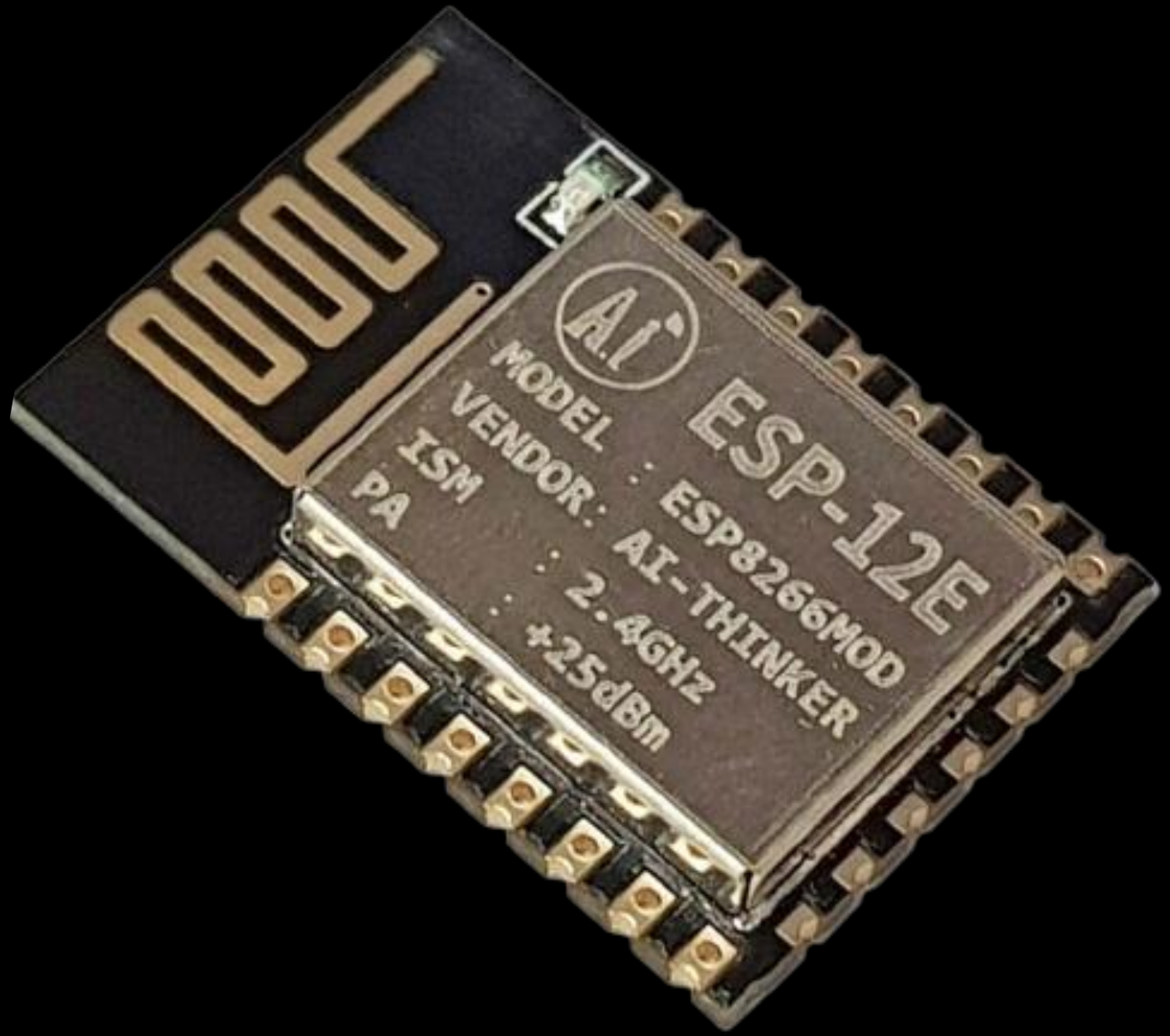

CA
Server
Reader cert
Web server cert
TLS tunnel
Card reader
Web server
Database

Card reader components


RFID reader
5 V PSU
ESP8266
Buzzer
RGB
RC522

ESP8266

- 32-bit RISC processor, 0.16 GHz
- 0.05 MB RAM
- 802.11 n support (2.4 GHz), up to 72.2 Mbps



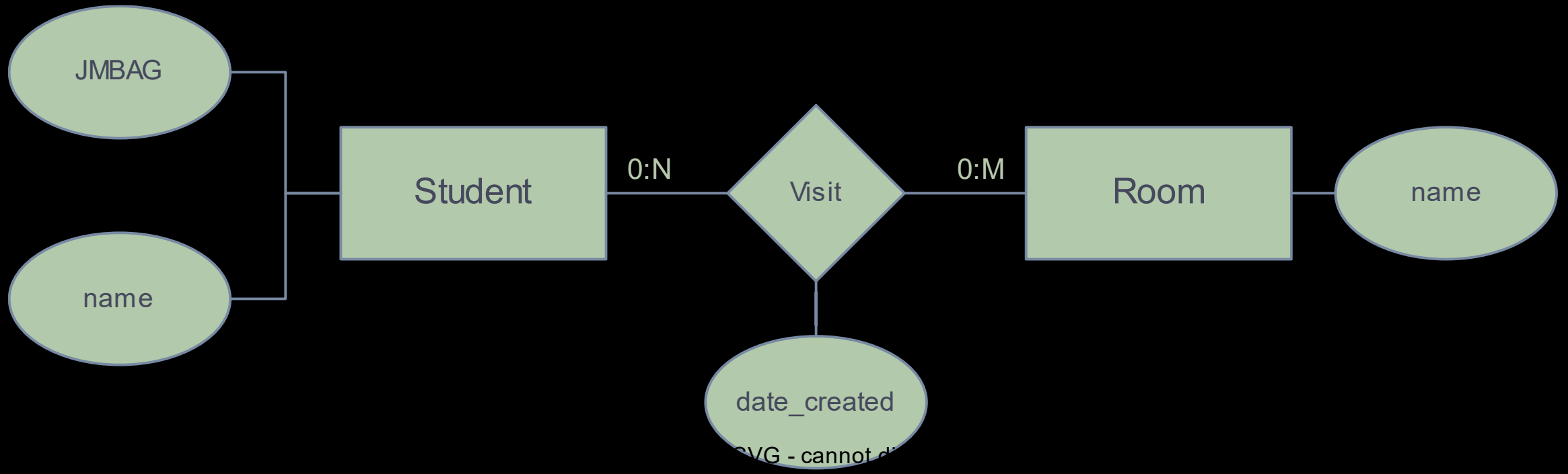
MFRC-522

- 13.56MHz RFID
- Works with the ISO 14443A standard tags
- SPI / I2C / UART

Server part


Dev
8080 HTTP
spring boot
HIBERNATE
H2

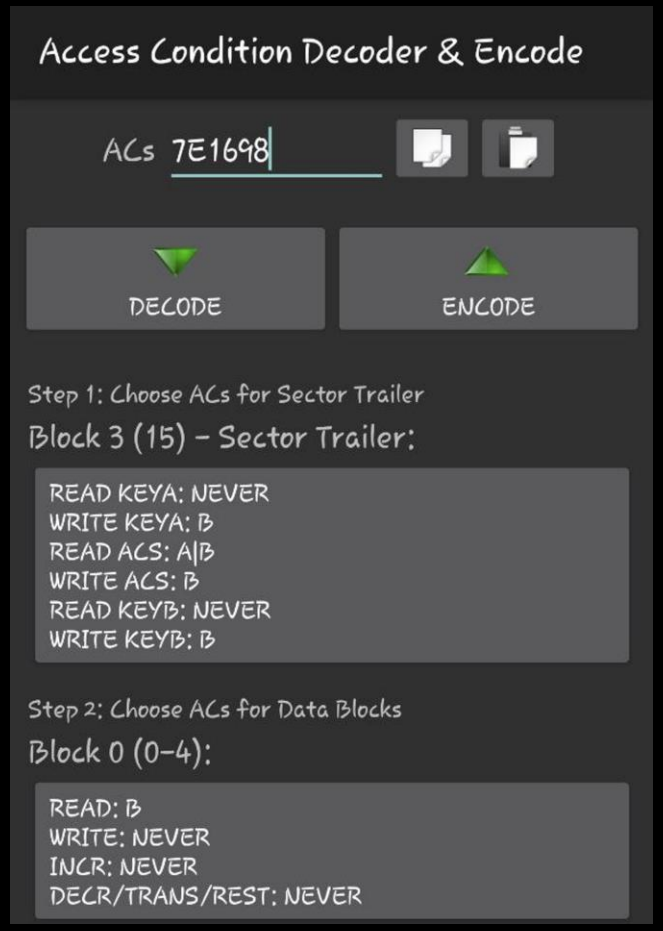
ERD

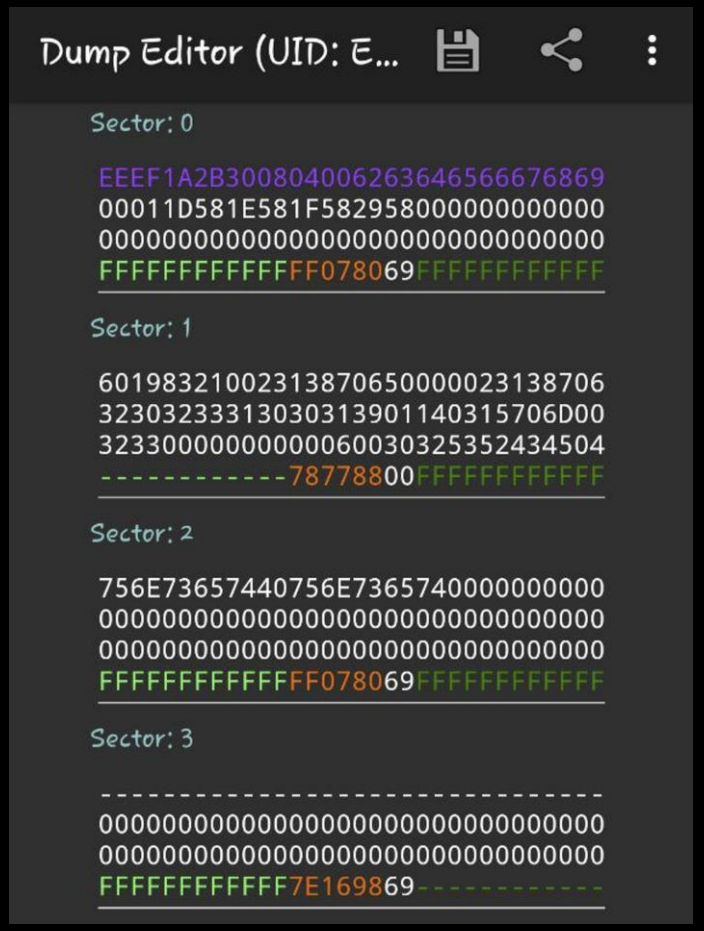


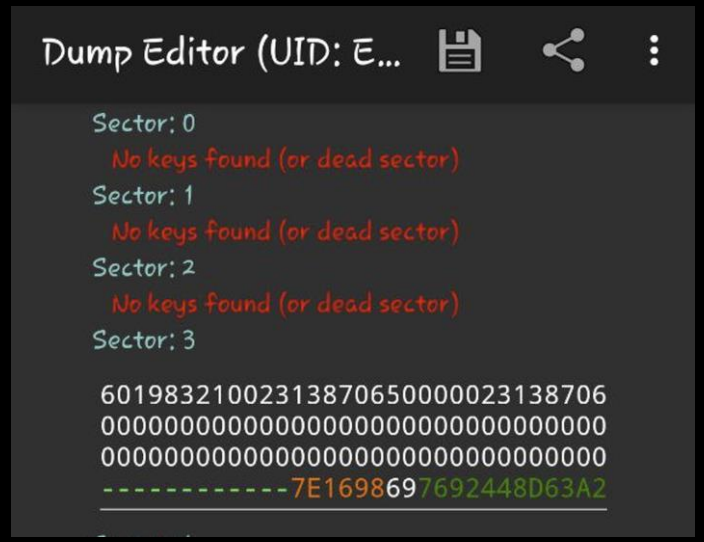
System Workflow

Tag configuration

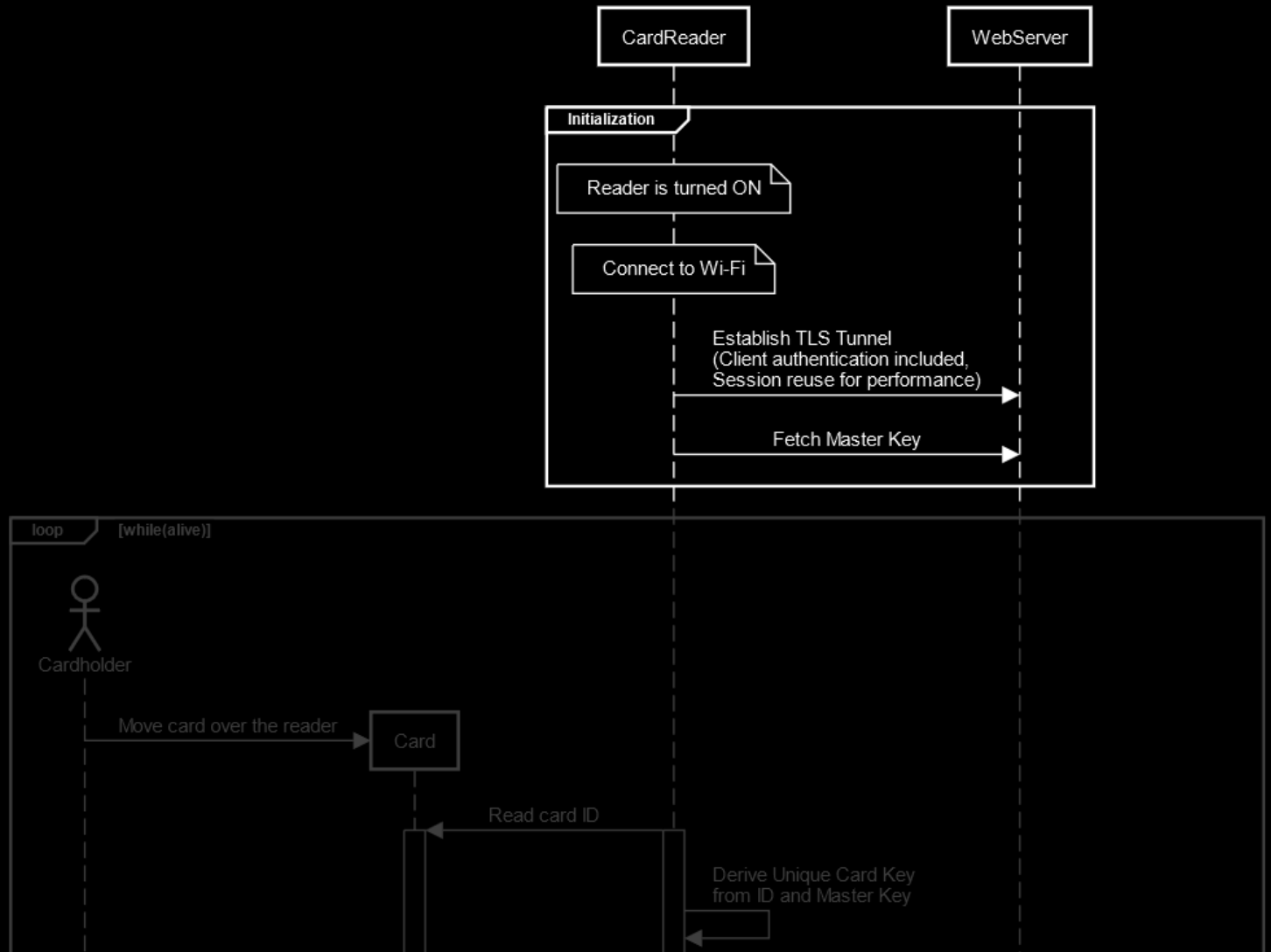
- MIFARE Classic Tool apk is used







Sequence diagram



https://sequencediagram.org/

Product DEMO

Challenges Faced

- Not all MFRC-522 modules work
- Smartphone requires root access to control UID
- MFRC-522 lacks emulation capability
- MFRC-522 library missing some modern features

Future Enhancements

- System vulnerable to the Wi-Fi jamming (Wiegand standard)
- Reader key interception
- ISO-14443A tags can be easily cracked
- Migration to the PN532 and using smartphone NFC capabilities

References

- Tutorial: how an RFID 13.56 Mhz read/write ISO-14443A tag works.
- Tag Memory access
- A 2018 practical guide to hacking NFC/RFID
- ESP8266EX Datasheet